EXHIBIT A

MICHIGAN STATE
UNIVERSITY

IDENTITY THEFT PREVENTION PROGRAM

I. ADOPTION

The Board of Trustees of Michigan State University adopted this Identity Theft Prevention Program ("Program") in compliance with the Red Flags Rule which implements Section 114 of the Fair and Accurate Credit Transactions (FACT) Act of 2003. The Red Flags Rule was jointly issued by the Federal Trade Commission, the federal bank regulatory agencies and the National Credit Union Administration with the underlying goal of detecting, preventing and mitigating identity theft. For purposes of this Program, identity theft is a fraud committed or attempted using personal identifying information of another person without authority. Several areas of the University engage in activities which are subject to the FACT Act and its Red Flags Rule.

II. PURPOSE

A. This Program is designed to provide guidelines for areas of the University (individually "Unit" and collectively "Units") that open or maintain one or more covered accounts. A covered account is a consumer account that involves or is designed to permit multiple payments or transactions, and any other account, including a business account, for which there is a reasonably foreseeable risk to customers or the safety and soundness of the University from identity theft.

The University opens and maintains covered accounts resulting from its participation in the Federal Perkins loan and Health Profession loan programs. Michigan State University also has covered accounts such as those arising from extending institutional loans to students, faculty and staff and offering deferred tuition and housing plans, Spartan Cash and recurring employee-requested payroll deductions for campus parking fees. The covered accounts referenced in this document are for illustrative purposes and do not reflect all of the University's covered accounts which are subject to the Red Flags Rule.

B. The Program is tailored to the University's size, complexity and nature of operations and will assist in reducing the risk of identity theft and minimizing potential damage from identity theft. Accepting credit cards for the payment of goods or services does not, in itself, make the University a creditor. The University is a creditor because it regularly extends or renews credit in connection with offering services to the University community.

C. Each Unit must determine whether its activities are subject to the Red Flags Rule and assess the risk of identity theft to its customers and the University. The risk-based assessment should include consideration of financial, operational, compliance, reputation and litigation risks.

III. PROGRAM ADMINISTRATION – UNIVERSITY RESPONSIBILITIES

A. Delegation and Oversight – The Board of Trustees of Michigan State University appoints the Controller of the University to oversee the development, implementation, and administration of the Program ("Program Administrator"). The Program Administrator may designate staff to assist with implementation of the Program and the Program Administrator is further authorized, if necessary, to amend and update the Program to reflect changing identity theft risks.

B. Program Administration – Administration of the Program will include, but is not limited to, the following:

1. Assisting Units with the identification of covered accounts and evaluating the risks of identity theft and the applicability of this Program to a Unit's operations;
2. Assisting Units with the identification, detection and mitigation of patterns, practices or specific activities, known as 'red flags' which may be indicative of attempts to engage in, or incidents of identity theft;
3. Assisting Units, as necessary, with an appropriate response to a red flag;
4. Assisting Units, as necessary, with the oversight of third party service providers that perform an activity for the University in connection with one or more covered accounts;
5. Training staff to implement the Program; and
6. Reviewing Unit reports related to red flags.

IV. UNIT RESPONSIBILITIES

A. Existence of Covered Accounts – Each Unit must determine whether it has covered accounts and the risk of identity theft related to those covered accounts.

B. Compliance Plan – Each Unit with covered accounts must develop and implement written policies and procedures to comply with the Program ("Unit Plan"). The Unit must provide a current version of its Unit Plan, including the types of covered accounts, to the Program Administrator annually and as otherwise requested.

C. Compliance Steward – Each Unit with covered accounts must designate a Red Flags Compliance Steward and provide his/her name, mailing address, e-mail address and telephone number to the Program Administrator. The Unit must inform the Program Administrator of any changes in the identity of, or contact information for, its Red Flags Compliance Steward. The Red Flags Compliance Steward will monitor the Unit's compliance with the Program and respond to all inquiries about the Unit's Plan.

D. Identify Relevant Red Flags

1. In order to identify relevant red flags, a Unit should consider the types of covered accounts it offers and maintains, methods used to open accounts, methods used to access covered accounts, and previous experiences with identity theft.

2. Using Attachment 1 as a reference, a Unit must identify, in writing, all red flags associated with the Unit's covered account activity.

3. Each Unit's description of red flags should be specific enough to enable the Unit's staff to identify them.

E. Detect Red Flags

1. Opening covered accounts – A Unit's Plan must include procedures to obtain identifying information about, and verify the identity of, a person opening a covered account. Identifying information means a name or number that may be used alone or in conjunction with any other information to identify a person including the name, date of birth, social security number, driver's license number, alien registration number, government passport number, employer or taxpayer identification number, or any other unique identification.

2. Existing covered accounts – A Unit's Plan must include procedures to detect red flags in connection with existing covered accounts such as authenticating customers, monitoring transactions and verifying the validity of change of address requests.

F. Respond to Red Flags

1. A Unit must respond to red flags in a manner that is commensurate with the degree of risk posed to prevent and mitigate identity theft.

2. In determining an appropriate response to red flags, the Unit should consider aggravating factors that may heighten the risk of identity theft, such as a data security breach which results in unauthorized access to a customer's account records, or notice that a customer has provided information related to a covered account held by the Unit to someone fraudulently claiming to represent the Unit or University or to a fraudulent website.

3. For illustrative purposes only, a Unit's response to red flags may include the following:
   a. Monitoring the covered account for evidence of identity theft;
   b. Contacting the customer;
   c. Changing any passwords 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. Closing an existing covered account;

g. Not attempting to collect on a covered account;

h. Notifying the Program Administrator of incidents of identity theft;

i. Notifying law enforcement after consulting the Program Administrator; and

j. Determining that no response is warranted under the particular circumstances.

G. Oversee Service Providers – A contract with a service provider to perform an activity in connection with one or more covered accounts must include a provision which requires the provider to have written policies and procedures designed to detect, prevent, and mitigate the risk of identity theft in compliance with the Red Flags Rule. The service provider must respond appropriately, after consulting with the Unit, to red flags.

H. Train Staff

1. At least annually and as the duties of staff change, the Unit will train or seek the assistance of others to train staff who are likely to handle covered accounts.

2. The following principles should be included in the Unit's training materials or programs:

a. Identity theft is a serious risk for consumers, the University, and third-party service providers that use or retain identifying information. It is necessary for the University to seek methods to minimize the potential threat of and harm from identity theft.

b. A person's identifying information should not be provided to anyone inside or outside the University who does not 'need to know' such information.

c. A person's identifying information may be stored in secure systems or facilities only if storage is necessary to perform a business function.

d. Reports or suspicions of identity theft should be handled as priority incidents, and immediate steps should be taken to remediate the resulting issues.

I. Update the Unit Plan – Each Unit with covered accounts should periodically review and update, if necessary, its Unit Plan to reflect changes in risks to customers or to the safety and soundness of the University from identity theft, arising from:

1. Experiences of identity theft;

2. Changes in methods to attempt identity theft;

3. Changes in methods to detect, prevent and mitigate identity theft;

4. Changes in the types of accounts that the Unit offers or maintains; and
5. Changes in the Unit's business arrangements.

J. Reporting

1. At least annually, each Unit with covered accounts must report on its compliance with the Red Flags Rule to the Program Administrator.

2. The report should address material matters related to the Unit's Plan and evaluate issues such as:
   a. The effectiveness of the Unit Plan in addressing the risk of identity theft in connection with opening covered accounts and with respect to existing covered accounts;
   b. Service provider arrangements; and
   c. Significant incidents of identity theft.

K. Reviewed

1. No changes warranted. M. Nelson, 25 February 2016.
2. No changes warranted. M. Nelson, 27 July 2017.

ATTACHMENT 1

EXAMPLES OF RED FLAGS

Direct Notification

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.

Suspicious Documents

2. Documents provided for identification appear to have been altered or forged.

3. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

4. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

5. Other information on the identification is not consistent with readily accessible information that is on file at the University, such as a signature card or recent check.

6. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

7. Personal identifying information provided is inconsistent when compared against external information sources used by the University. For example, the address does not match any address in the consumer report.

8. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.

9. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the University. For example:
   a. The address on an application is the same as the address provided on a fraudulent application; or
   b. The phone number on an application is the same as the number provided on a fraudulent application.

10. The social security number provided is the same as that submitted by other persons opening an account or other customers.

11. The address or phone number provided is the same as or similar to the address or phone number submitted by an unusually large number of other persons opening accounts or other customers.

12. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

13. Personal identifying information provided is not consistent with personal identifying information that is on file with the University.

14. For Unit or University activities that use 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.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

15. Shortly following the notice of a change of address for a covered account, the University receives a request for a new, additional, or replacement account, card, or cell phone, or for the addition of new authorized users on the account.

16. A covered account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment, or makes an initial payment, but no subsequent payments.

17. 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 or services;
    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 phone call patterns in connection with a cellular phone account.

18. 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).

19. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

20. The University is notified that the customer is not receiving paper account statements.

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

Alerts, Notifications or Warnings from a Consumer Reporting Agency

22. A fraud or active duty alert is included with a consumer report.

23. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

24. A consumer reporting agency provides a notice of address discrepancy.

25. 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 the University.