ATTACHMENT 1
EXAMPLES OF RED FLAGS
Copied From the MSU Identity Theft Prevention Program

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; or
    d. An account that was closed for cause or identified for abuse of account privileges by the University.