Clarion University
Identity Theft Prevention Program

A) Purpose

The purpose of the Identity Theft Prevention Program (Program) is to detect, prevent and mitigate identity theft in connection with any "covered" account at the university. The Program will

- Identify the risks for new and existing "covered accounts" the university maintains for students and staff
- Detect activities (aka "red flags") that raise suspicion of fraudulent activity
- Respond appropriately to any "red flags" that are detected to prevent and mitigate identity theft
- Establish guidelines and protocol for periodic review and update of the program.

This Program was developed in alignment with the Federal Trade Commission Identity Theft Red Flags rule.

B) Definitions

Covered Account:

- Any accounts that constitute a continuing financial relationship between the university and a person for a service, or that are designed by their nature to permit multiple payments or transactions deferred payment arrangements, or extensions of credit, loans, or deposit accounts. These types of accounts include student loans and student payment plans administered by the university or a contracted Service Provider.
- Any other account the university offers or maintains for which there is a reasonably foreseeable risk to holders of the account or to the safety and soundness of the university from identity theft.

Service Provider: An outside entity engaged by the university to perform an activity in connection with one or more Covered Accounts.

Identity Theft: Fraud committed or attempted using the identifying information of another person

Red Flag A pattern, practice or specific activity that indicates the possible existence of Identity Theft that occurs with a Covered Account at the university.

C) Program Scope, Administration, and Updates

1. In order to identify relevant Red Flags, the university considers the types of Covered Accounts it offers or maintains, the methods it provides to open its Covered Accounts, the methods it provides to access its Covered Accounts, and its previous experiences with Identity Theft.

2. University Covered Accounts include Student Federal Loans (Direct, PLUS, Perkins), university Book Loans, Deferred Tuition Payments, and Student Records with Social Security Numbers.

3. This Program applies to all university employees, faculty, students and university vendors or other Service Providers that have, or are granted access to, Covered Accounts

4. The President's Executive Council has designated the Associate Vice President for Computing Services as Identity Theft Prevention Program Administrator responsible for the oversight of the Program. Oversight responsibilities include the development and coordination of the Program and the identification of Department Managers and Service Providers for areas that work with Covered Accounts. Oversight responsibilities also include an annual review of the Program to assess the university's experiences with identity theft, changes in identity theft methods, changes in identity theft detection and prevention methods, changes in types of Covered Accounts the university maintains and changes in the university's business arrangements with Service Providers. Based on this assessment, the program will be revised as appropriate subject to approval of the President's Executive Council.

5. Designated Covered Account Department Managers are responsible for the operational implementation of the Program within their departments including staff training, risk assessment and red flag detection, incident response coordination, and reporting.

a. Based on the current assessment of Covered Accounts, the following Designated Account Department Managers have been identified:

- Computing Services Manager of Application Services
- Associate Vice President of Enrollment Management (Undergraduate and Graduate Admissions)
- Director of Student Financial Services
- Registrar

D) Identification and Detection of Red Flags

A "Red Flag" is a pattern, practice, or specific activity that indicates the possible existence of identity theft. The following categories are identified as red flags:

- Alerts, notifications or warnings from a consumer reporting agency including fraud alerts, credit freezes or official notice of address discrepancies.
- The presentation of suspicious documents such as those appearing to be forged or altered.
- The presentation of suspicious personal identifying information such as a photograph or physical description on the identification that is not consistent with the appearance of the person presenting the identification; discrepancies in address, Social Security Number, Student ID, Employee Id, or other information on file,; and/or failure to provide all required information.
- Unusual use or suspicious account activity that would include material changes in payment patterns, notification that the account holder is not receiving mailed statement, or that the account has unauthorized charges;
- A request to mail something to an address that is not on file.
- Notice received from students, victims of identity theft, law enforcement, other persons regarding possible identity theft in connection with Covered Accounts.

Appendix A contains a detailed list of potential Red Flags.

Departments shall address the detection of Red Flags in connection with the opening or maintenance of Covered Accounts, such as:

- Obtaining identifying information about, and verifying the identity of, a person opening/closing/changing a Covered Account; and
- Authenticating customers, monitoring transactions, and verifying the validity of change of address requests in the case of existing Covered Accounts.

E) Response to Red Flags

Any time an employee suspects a potential Red Flag, the employee should assume that this Identity Theft Prevention Program applies and immediately report the Red Flag details to the Department Manager who in turn will escalate the issue to the Identity Theft Prevention Program Administrator.

Further, if a transaction is suspected to be fraudulent, the department must immediately take appropriate actions. Actions may include:

1. Refuse to take any further action with the Covered Account and cancel any related transactions.
2. Revoke access to university systems via removing access to potentially compromised system credentials
3. Continue to monitor a Covered Account for evidence of Identity Theft.

The Department Manager and the Identity Theft Prevention Program Administrator will identify other appropriate follow-up actions to include contacting other university departments, contacting the individual, and/or contacting law enforcement.

F) Service Provider Arrangements

In the event the university engages a Service Provider to perform an activity in connection with one or more Covered Accounts, the university will select and retain service providers that can maintain appropriate safeguards. Selected vendors will be required by contract to implementation and maintain such safeguards.

Appendix A – "Red Flag" Examples

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

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 that 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 financial institution or creditor, 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.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. 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.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the university. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or
b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

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

16. 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.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the university.

18. 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

19. Shortly following the notice of a change of address for a Covered Account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:
    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 Financial Institution or Creditor

26.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.