Policy: Identity Theft Prevention Policy & Program	**Policy Number:** I-7.8
Policy Owner(s): Human Resources	**Original Date: 4/23/2019**
Last Revised Date: 1/14/2020	**Approved Date: 2/26/2020**

I. **POLICY**: John Carroll University ("the University") adopts this policy as part of its program for the prevention of Identity Theft. Consistent with the Red Flag rule under the Fair and Accurate Credit Transactions Act ("FACT Act"), the University has established an Identify Theft Program ("the Program") with reasonable policies and procedures to detect, identify, and mitigate Identity Theft in its Covered Accounts. The University has adopted this Identity Theft Prevention Policy to incorporate relevant Red Flags into a Program to enable the University to detect and respond to potential Identity Theft. The University will update the Program periodically to reflect changes in risks to Customers, creditors or the University from Identity Theft.

II. **PURPOSE**: The University recognizes that some activities of the University are subject to the provisions of the FACT Act and its "Red Flag" rule. This law requires that a Red Flag policy (from which a Red Flag program will be developed) be adopted, with oversight of the program assigned to a senior management level administrator and with regular program reviews. Therefore, the University adopts the following Identify Theft Prevention Policy and Program.

III. **SCOPE**: All John Carroll University employees

IV. **DEFINITIONS:**

Red Flag rule definitions used in this policy and Program:

Account: a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household, or business purposes. It includes: (1) an extension of credit, such as the purchase of property or services involving a deferred payment, and (ii) a deposit account.

Covered Accounts:

- Any Account the University offers or maintains primarily for personal, family or household purposes that involves multiple payments or transactions, and/or

- Any other account the University offers or maintains for which there is a reasonably foreseeable risk to Customers or to the safety and soundness of the University from Identity Theft.
- Primary Covered Accounts Maintained by JCU
    1. Student Financial Accounts
    2. Payment Plan Agreements
    3. Institutional Loans and Accounts

Credit: The right granted by a creditor to a debtor to defer payment of debt or to incur debt and defer its payment or to purchase property or services and defer payment.

Creditor: An entity that regularly extends, renews, or continues credit.

Customer: Any person with a Covered Account with a creditor. In the University context, the most common example of a Customer would be a student with a financial account with the University.

Identifying Information: Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including:

1. Name
2. Address
3. Telephone number
4. Social security number
5. Date of birth
6. Government issued driver's license or identification number
7. Alien registration number
8. Government passport number
9. Employer or taxpayer identification number
10. Unique electronic identification number
11. Computer's Internet Protocol address

Identity Theft: A fraud committed or attempted using the Identifying Information of another person without authority.

Program: The University's Identity Theft Prevention Program

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

V. <u>GUIDELINES</u>:

A. **Program Administrator**- the Vice President for Finance and Administration, or designee, is designated as the Program Administrator for the Identity Theft Prevention Program. The Program Administrator shall exercise appropriate and effective

oversight over the Program and shall report regularly to senior University leadership on the Program.

B. **Program Administration and Maintenance**

1. The Program Administrator is responsible for developing, implementing and updating the Program. The Program Administrator, in coordination with the Office of Legal Affairs, the Business Office, and the Information Technology Services Department, will be responsible for ensuring appropriate training of University staff on the Program; for reviewing any staff reports regarding the detection of Red Flags and the steps for identifying, preventing and mitigating Identity Theft; determining which steps of prevention and mitigation should be taken in particular circumstances; and considering periodic changes to the Program.

2. The Program will be periodically reviewed and updated to reflect changes in Identity Theft risks and changes in technology. The Program Administrator will consider the University's experiences with Identity Theft; changes in Identity Theft methods; changes in Identity Theft detection, mitigation and prevention methods; changes in types of accounts the University maintains; changes in the University's business arrangements with other entities; and any changes in legal requirements in the area of Identity Theft. After considering these factors, the Program Administrator will determine whether changes to the Program, including the listing of Red Flags, are warranted.

3. The Program Administrator shall confer with the Office of Legal Affairs, the Information Technology Services Department, and other University personnel as necessary to ensure compliance with the Program. The Program Administrator shall regularly report to senior University leadership on the effectiveness of the Program. The Program Administrator shall present any recommended changes to the senior University leadership for approval.

C. **Identification of Red Flags-** In order to identify relevant Red Flags, the University considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The following are relevant Red Flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

1. Notifications and Warnings from Credit Reporting Agencies

    a) Report of fraud accompanying a credit report;
    b) Notice or report from a credit agency of a credit freeze on a Customer or applicant;
    c) Notice or report from a credit agency of an active duty alert for an applicant;
    d) Receipt of a notice of address discrepancy in response to a credit report request; and/or
    e) Indication from a credit report of activity that is inconsistent with a Customer's usual pattern or activity.

2. Suspicious Documents

    a) Identification document or card that appears to be forged, altered or inauthentic;
    b) Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the documentation;
    c) Other document with information that is not consistent with existing Customer information (such as if a person's signature on a check appears forged); and/or
    d) Application for service that appears to have been altered or forged.

3. Suspicious Personal Identifying Information

    a) Identifying Information presented that is inconsistent with other information the Customer provides (example: inconsistent birth dates);
    b) Identifying Information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
    c) Identifying Information presented that is the same as information shown on other applications that were found to be fraudulent;
    d) Identifying Information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
    e) Social security number presented that is the same as one given by another Customer;
    f) An address or phone number presented that is the same as that of another person;
    g) A person fails to provide complete personal Identifying Information on an application when

reminded to do so (however, by law social security numbers must not be required); and/or

h) A person's Identifying Information is not consistent with the information that is on file for the Customer.

4. Suspicious Account Activity or Unusual Use of Account

a) Change of address for an account followed by a request to change the account holder's name;
b) Payments stop on an otherwise consistently up-to-date account;
c) Account used in a way that is not consistent with prior use (example: very high activity);
d) Mail sent to the account holder is repeatedly returned as undeliverable;
e) Notice to the University that a Customer is not receiving mail sent by the University;
f) Notice to the University that an account has unauthorized activity;
g) Breach in the University's computer system security; and/or
h) Unauthorized access to or use of Customer account information.

5. Alerts from Others- Notice to the University from a Customer, Identity Theft victim, law enforcement or other person that it has opened or is maintaining a fraudulent account for a person engaged in Identity Theft.

D. **Detecting Red Flags**- The Program's general Red Flag detection practices are described in this policy. The Program Administrator, in conjunction with the Office of Legal Affairs, the Business Office, and Information Technology Services, will develop and implement specific methods and protocols appropriate to meet the requirements of this Program.

1. New Accounts- In order to detect any of the Red Flags identified above associated with the opening of a new account, University personnel will take the following steps to obtain and verify the identity of the person opening the account:

a) Require certain identifying information such as name, date of birth, residential or business address, driver's license or other identification;
b) Verify the Customer's identity by a reasonable procedure (for instance, by review of a photo

identification such as a driver's license, student identification, or other state-issued identification card); and/or

c) Independently contact the Customer.

2. Existing Accounts- In order to detect any of the Red Flags identified above associated with existing accounts, University personnel will take the following steps to obtain and verify the identity of the person on an existing account:

a) Verify the identification of Customers if they request information (in person, via telephone, via facsimile, via email);
b) Verify the validity of requests to change billing addresses; and/or
c) Verify changes in banking information given for billing and payment purposes.

E. **Responding to Red Flags and Mitigating Identity Theft-** In the event a University employee detects any identified Red Flags, such employee shall take all appropriate steps to respond and mitigate Identity Theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to the following examples:

1. Immediate discussion with supervisor regarding concerns and/or reports;
2. Continue to monitor an account for evidence of Identity Theft;
3. Contact the Customer;
4. Change any passwords or other security devices that permit access to accounts;
5. Not open a new account;
6. Close an existing account;
7. Reopen an account with a new number;
8. Notify JCU Police Department or other law enforcement;
9. Consider other security measures to address any Identity Theft and/or prevent future Identity Theft;
10. Take corrective measures to address any Identity Theft that may have resulted from the University's processes, actions or inactions;
11. Determine that no response is warranted under the particular circumstances, and/or
12. Notify credit reporting agencies.

F. Staff Training and Reporting- University employees responsible for implementing the Program shall be trained under the direction of

the Program Administrator, or designee, in the detection of Red Flags, and the responsive steps to be taken when a Red Flag is detected.

Such employees are expected to notify the Program Administrator, or designee, once they become aware of an incident of Identity Theft. On a regular basis, University employees responsible for the development, implementation, and administration of the Program shall report to the Program Administrator on the University's compliance with the Program. The report should address such issues as effectiveness of the policies and procedures in addressing the risk of Identity Theft in connection with the opening and maintenance of Covered Accounts; service provider agreements; significant incidents involving Identity Theft and the University's response; and recommendations for changes to the Program.

G. **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 take the steps necessary to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of Identity Theft. Request copy of service provider's policy in regards to Identity Theft to ensure compliance with applicable Federal Law.

VI. **CROSS REFERENCE**:

Sensitive Data and Security Policy