Policy Title: Identity Theft Prevention Policy
Policy Summary: Identification, Detection and Response to Potential or Confirmed Instances of Identity Theft and Reporting Confirmed or Suspected 'Red Flag' Incidents When Detected
Policy Category: Financial
Policy Owner: Finance

Policy Summary

This policy describes 1) the process that Drake University uses to identify, detect, and respond to instances of potential or confirmed identity theft related to any of the covered accounts listed in this policy and 2) provides information on reporting confirmed or suspected 'Red Flag' incidents when detected.

Purpose

The Drake University Identity Theft Prevention Policy is designed to reduce the risk of identity theft through detection, prevention and mitigation of patterns, practices or activities related to covered accounts ("Red Flags") that could be indicative of potential identity theft. The Fair and Accurate Credit Transactions Act (FACTA) of 2003 contains program requirements at 16 CFR 681, including the "Red Flag Rule" in sections 114 and 315, and is enforced by the Federal Trade Commission (FTC). The Chief Financial Officer (CFO) is responsible for implementing an identity theft prevention program and ensuring compliance with the Identity Theft Prevention Policy and may delegate day-to-day management to others as appropriate.

Scope

This policy applies to all University departments that collect and maintain personal information associated with any of the Covered Accounts listed in this policy.

Definitions

Covered Account means (i) an account that Drake University offers or maintains primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions and (ii) any other financial account that the University offers or maintains for which there is a reasonably foreseeable risk of identity theft to the customer (i.e. students, parents and/or patients).

Identity Theft means fraud that involves stealing money or getting other benefits by using the identifying information of another person.

Notice of an Address Discrepancy means a notice that a credit bureau sends to Drake University. Mail returned because of improper address is not a Notice under this policy.

Personally Identifiable Information is any piece of information which may be used to uniquely identify, contact, or locate an individual. This includes, but is not limited to, taxpayer identification numbers, driver's license numbers, passport identification numbers, student identification numbers, passwords, PINs, personal account numbers, computer accounts and passwords, protected health information, financial information, home address or phone

numbers and/or any combination of information that will uniquely identify an individual.

Red Flag means a pattern, practice or specific activity that indicates the possible existence of identity theft.

Service Provider means a vendor that provides services directly to Drake University related to Covered Accounts.

Policy

Covered Accounts:
Covered Accounts maintained by Drake University include but are not limited to the following:

1. Student loans (including Federal Perkins Loans, short-term emergency loans and any other private loans lent by the University to students)
2. Student accounts (including Bulldog Bucks)
3. Patient accounts with the Student Health Office
4. Any other University records related to Covered Accounts that contain Personally Identifiable Information

Identifying Red Flags:
Drake University will identify and respond to Red Flags that may indicate potential identity theft.

Red Flags include but are not limited to the following:

1. Alerts, notifications or warnings from a consumer reporting agency, including notices of credit freezes, Notices of Address Discrepancies, and receipts of consumer reports showing patterns of activities that are inconsistent with the history and usual pattern of activity of the account holder.
2. Address discrepancies that cannot be explained. Changing an address more than once a year or changing a direct deposit account for refunds more than once a year would not be considered a red flag action at the University when done through MyDUSIS. However, it might constitute suspicious activity at a financial institution whose account holders do not change residences as often as university students.
3. Suspicious documents, including: a) photographs or physical descriptions that are inconsistent with the individual presenting the document; b) incomplete, altered, forged, or inauthentic documents; or c) other personal identifying information that is inconsistent with information on file with the University.
4. Complaints or questions from students, guardians, or customers about charges to a covered account for goods/services they claim were never received.
5. Suspicious activity related to Covered Accounts including, but not limited to:
    a. stopping payments on an otherwise consistently up-to-date account;
    b. unusual use of accounts that have been previously inactive for a lengthy period of time,
    c. mail being returned as undeliverable although transactions continue to be conducted in connection with the covered account; or
    d. unauthorized account changes or transactions.
6. Notice from customers, victims of identity theft, law enforcement authorities or other individuals regarding possible identity theft in connection with University Covered Accounts.

Detecting Red Flags:

1. The following actions will be taken, as appropriate, to confirm the identity of students and other customers when they open and/or access Covered Accounts:
    a. Obtain appropriate personal identifying information (e.g. photo identification, date of birth, academic status, user name and password, address, etc.) prior to opening or allowing access to a covered account; or prior to issuing a new or replacement ID card.
    b. When certain changes are made to Covered Accounts online, the account holder will receive notification to confirm the change is valid.
    c. Verify the accuracy of changes made to Covered Accounts that appear to be suspicious.
2. Information systems containing Covered Account information will be monitored by Information Technology Services (ITS) for the Student Information System (SIS) to detect any unusual user activity that could indicate improper access to and/or use of consumer information.
3. Information Technology Services will implement appropriate information technology controls to reduce the potential for inappropriate access including but not limited to access controls, multi-factor authentication, email filtering, etc.

Responding to Red Flags:

Any staff member encountering a Red Flag will assess the situation to determine if potential identity theft exists. The assessment may determine that no risk of identity theft is present (i.e. a mistake has occurred, or the occurrence is readily explainable). If, after preliminary investigation, the employee suspects identity theft may have occurred, he/she will notify the CFO or Designee. The CFO/Designee will further investigate the matter, and, if identity theft is confirmed, may take the following actions in coordination with the department managing the Covered Account to mitigate harm, as appropriate, based on the individual circumstances:

1. Notify Campus Public Safety
2. Notify the covered account holder if the holder is the identity theft victim
3. Notify the Financial Aid Office and the lending institution(s) for student loans, if applicable
4. Notify the third-party student loan Service Provider(s), if applicable
5. Notify the Student Accounts Office and collection agencies handling delinquent accounts, if applicable
6. Notify the consumer reporting agency(ies) about address discrepancies associated with credit reports received
7. Notify appropriate law enforcement units
8. File a report with the local police department
9. Correct any erroneous information associated with the account
10. Establish Red Flag alerts to notify relevant employees of suspected identity theft (e.g. notes in Covered Account information systems or files, etc.)

The University department responsible for the Covered Account may take the following actions, based on the individual circumstances:

1. Notify the student or individual account holder of the evidence of identity theft and monitor the account for additional fraudulent activity

2. Request additional information as required to verify identity
3. Work with ITS to change passwords and security codes as appropriate to further secure access to the account
4. Reopen a covered account with a new account number, close an existing account, and decline to open a new covered account as appropriate
5. Attempt to identify the source of the Red Flag and take appropriate steps to prevent additional identity thefts

Oversight of Service Providers:
Drake University may contract with vendors to provide services related to Covered Accounts. The contracting department will maintain written certification from the vendor stating it complies with FACTA Red Flag Rule regulations. The department will investigate any service provider occurrences indicating a potential lack of compliance, and take any necessary actions to mitigate potential risk.

Program Education:
On an annual basis, all departments managing Covered Accounts will provide education to current staff members and new hires on this policy and any internal department procedures created to implement it.

Program Assessment and Reporting:
An identity theft prevention program report will be forwarded through the CFO to the President and the Audit Committee of the Board of Trustees annually. The report will contain:

1) a summary of Red Flag Rule monitoring activities;
2) a description of any identity theft incidents that have occurred and the response to them;
3) any recommended identity theft prevention program changes; and
4) any recommended changes to this Identity Theft Prevention Policy.

The Audit Committee of the Board of Trustees will approve material changes to the Identity Theft Prevention policy.

Resources and Related University Policies:

- "Red Flag Rule", Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003, 16 CFR subsection 681, as enforced by the Federal Trade Commission (FTC).
- Gramm-Leach Bliley Act.
- Iowa Code Title XVI, Chapter 715C Personal Information Security Breach Protection.
- Family Education Rights and Privacy Act (FERPA) statement.