Identity Theft Policy

Section 1: Background

The risk to Dickinson College (the “College”), its employees and students from data loss and identity theft is of significant concern to the College and can be reduced only through the combined efforts of every employee and contractor that accesses certain types of student accounts.

Section 2: Purpose

The College adopts this Identity Theft Policy to help protect students and the College from damages related to the loss or misuse of information contained in certain covered accounts.

This policy will:

1. Identify "red flags" (patterns, practices and activities that signal possible identity theft);
2. Describe ways to detect these red flags;
3. Describe appropriate responses to detected red flags to prevent and mitigate identity theft;
4. Describe appropriate responses to the receipt by the College of address discrepancy notices from national consumer credit reporting agencies; and
5. Ensure that this Policy is updated periodically to reflect changes in risks.

Section 3: Scope

This Identity Theft Policy applies to employees, contractors, consultants, temporary workers, and other workers at the College that have access to certain student accounts.

Section 4: Covered Accounts

This Identity Theft Policy is designed to protect certain types of student and employee accounts maintained by the College. Every new and existing student or employee account that meets the following criteria is covered by this Policy:

1. Any account that the College offers to students or employees that involves or is designed to permit multiple payments or transactions; or
2. Any other student or employee account offered or maintained by the College for which there is a reasonably foreseeable risk to students, employees or to the safety and soundness of the College from identity theft, including financial, operational, compliance, reputation or litigation risks.
Section 5: Red Flags

5.A: Credit Reporting Agency Notifications

5.A.1: The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification.

1. Alerts, notifications or warnings from a consumer credit reporting agency;
2. A fraud or active duty alert included with a consumer credit report;
3. A notice of credit freeze from a consumer credit reporting agency in response to a request for a consumer report; or
4. A notice of address discrepancy from a consumer credit reporting agency.

5.A.2: Red flags also include consumer credit reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an account holder, such as:

- A recent and significant increase in the volume of inquiries;
- An unusual number of recently established credit relationships;
- A material change in the use of credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a financial College or creditor.

5.B: Suspicious documents

5.B.1: Documents provided for identification that appear to have been altered or forged.

5.B.2: The photograph or physical description on the identification is not consistent with the appearance of the account holder presenting the identification.

5.B.3: Other information on the identification is not consistent with information provided by the person opening a new covered account or account holder presenting the identification.

5.B.4: Other information on the identification is not consistent with readily accessible information that is on file with the College, such as a signature card or a recent check.

5.B.5: An application, admission documentation or other covered account document appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

5.C: Suspicious personal identifying information

5.C.1: Personal identifying information provided is inconsistent when compared against external information sources used by the College. For example:
• The address does not match any address in the consumer credit report;
• The Social Security number (SSN) has not been issued or is listed on the Social Security Administration’s Death Master File; or
• Personal identifying information provided by the account holder is not consistent with other personal identifying information provided by the account holder. For example, there is a lack of correlation between the SSN range and date of birth.

5.C.2: Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the College. For example, the address on an application, admission form or other document is the same as the address provided on a fraudulent application.

5.C.3: Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the College. For example:

- The address on an application, admission form or other covered account document is fictitious, a mail drop, or a prison; or
- The phone number is invalid or is associated with a pager or answering service.

5.C.4: The SSN provided is the same as that submitted by other account holders.

5.C.5: 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 account holders.

5.C.6: The account holder fails to provide all required personal identifying information on admission forms or other College documents, or in response to notification that such documents are incomplete.

5.C.7: Personal identifying information provided is not consistent with personal identifying information that is on file with the College.

5.C.8: When using security questions (mother’s maiden name, pet’s name, etc.), the person opening the covered account cannot provide authenticating information beyond that which generally would be available from a wallet or consumer credit report.

5.D: Unusual use of, or suspicious activity related to, the covered account

5.D.1: A covered account is used in a manner commonly associated with known patterns of fraud patterns. For example, the account holder fails to make the first payment or makes an initial payment but no subsequent payments.

5.D.2: A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

- Nonpayment when there is no history of late or missed payments;
- Any other material change in payment patterns.
5.D.3: Mail sent to the account holder is returned repeatedly as undeliverable although payments/transactions continue to be conducted in connection with the account holder's covered account.

5.D.4: The College is notified that the account holder is not receiving paper account statements.

5.D.5: The College is notified of unauthorized charges or transactions in connection with an account holder's covered account.

5.D.6: The College receives notice from account holders, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the College.

5.D.7: The College is notified by an account holder, 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.

Section 6: Responding to Red Flags

6.A: Once potentially fraudulent activity is detected, an employee of the College must act quickly as a rapid appropriate response can protect account holders and the College from damages and loss.

6.A.1: Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the Designated Authority identified in Section 8.A.3 hereof for determination.

6.A.2: The Designated Authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

6.B: If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1. Canceling the transaction and/or closing the account;
2. Notifying and cooperating with appropriate law enforcement;
3. Determining the extent of liability of the College; and
4. Notifying the account holder that fraud has been attempted.

Section 7: Periodic Updates to Plan
7.A. Every two years, the Board of Trustees directs the Vice President for Finance and Administration, with oversight as necessary or advisable from the Committee on Finance, Budget and Audit, to determine whether all aspects of the Policy are up to date and applicable in the current business environment. The Vice President for Finance and Administration, at his/her discretion, or upon recommendation of the Committee on Finance, Budget and Audit, may re-evaluate the Policy more frequently if he, she or the Committee on Finance, Budget and Audit determines that such re-evaluation is warranted due to changing risks or prevalent detection of fraudulent activity with respect to covered accounts.

7.B: Periodic reviews will include an assessment of which accounts are covered by the Policy.

7.C: As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

7.D: Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the College and its students.

**Section 8: Program Administration**

8.A: Involvement of management

1. The Identity Theft Prevention program shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.
2. The Identity Theft Prevention Program is the responsibility of the Board of Trustees. Approval of the initial plan must be appropriately documented and maintained.
3. Operational responsibility of the program is delegated to the Vice President for Finance and Administration (the "Designated Authority").

8.B: Staff training

1. Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the College, its students and employees.
2. The Designated Authority is responsible for ensuring identity theft training for all requisite employees and contractors.
3. Employees with access to covered accounts must receive annual training in all elements of this policy.
4. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

8.C: Oversight of service provider arrangements

1. It is the responsibility of the College to ensure that the activities of all service providers that have access to covered accounts are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
2. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

Section 9: Address Discrepancies in Consumer Credit Reports

9.A: Applicability

1. This Section 9 applies in the event that the College utilizes consumer credit reports.
2. If the College requests a consumer credit report regarding a student or employee, and if the address in such request differs from the address that the applicable consumer credit reporting agency has on file for such individual, the credit reporting agency will issue a Notice of Address Discrepancy to the College.
3. If and when the College receives a Notice of Address Discrepancy, the provisions of Section 9.B below shall apply.

9.B: Duties regarding address discrepancies

1. Upon receipt of a Notice of Address Discrepancy, the College must take steps that will enable the College to reasonably believe that a credit report relates to the student or employee for whom it was requested. The College may reasonably confirm that an address is accurate by any of the following means:
   a. Verification of the address with the student or employee;
   b. Review of other College records that contain the individual's address;
   c. Verification of the address through third-party source; or
   d. Other reasonable means as determined by the College from time to time.
2. If an accurate address is confirmed, the College shall furnish the individual's address to the nationwide consumer reporting agency from which it received the Notice of Address Discrepancy if:
   a. The College establishes a continuing relationship with such individual; and
   b. The College, regularly and in the ordinary course of business, furnishes information to the consumer reporting agency.

If an accurate address cannot be confirmed, then the credit report received cannot be used with respect to the individual for whom it was requested. The College should advise the individual in question of the address discrepancy and the inability to confirm an accurate address by the College and the applicable credit reporting agency, and the College should advise the individual to take such steps as are necessary to rectify the discrepancy.
Related Information

History/Revision Information

Responsible Office/Division:

Effective Date: May 1, 2009

Last Amended Date: April 25, 2009

Next Review Date:

Also Found In: Minutes of the Trustee Committee on Finance, Budget and Audit