SECTION 1500.03
IDENTITY THEFT PREVENTION PROGRAM (RED FLAG)

Purpose:
To establish an Identity Theft Prevention Program designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the program in compliance with Part 681 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA) of 2003.

Scope of Covered Activities/Business Processes, Rules:
Any account or financial service that Lake Region State College offers or maintains for which there is reasonably foreseeable risk to customers or to the safety and soundness of Lake Region State College from identity theft, including financial operational, compliance, reputation, or litigation risks.

Related Documents/Policies:
SBHE Policy 1901.2 Computing Facilities
SBHE Policy 1912 Public Records
Lake Region State College PCI (Payment Card Industry) Policy
Lake Region State College Information Security Response Policy
Lake Region State College Customer Information Safeguarding Program
NDUS Policy 511 Student Criminal History Background Checks and corresponding Procedure 511
NDUS Policy 602.3 Job Applicant/Employee Criminal History Background Checks and corresponding procedure 602
NDUS Policy 1912 Public Records; Procedure 1912.1 Information Security Procedures
NDUS Procedure 1912.2 Student Records – Directory Information
NDUS Procedure 1912.3 Employee Personal Information
SBHE Policy 802.7

Definitions:
Identity Theft - Fraud committed or attempted using the identifying information of another person without authority.
Covered Account - An account that Lake Region State College offers or maintains primarily for personal or business purposes that involves or is designed to permit multiple payments or transactions. Covered accounts includes but is not limited to Student ID Card, credit/debit card processing, financial aid information, student loan information, business accounts, payroll account information; and any other account that Lake Region State College offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of Lake Region State College from identity theft, including financial operational, compliance, reputation, or litigation risks.
Red Flag - A pattern, practice, or specific activity that indicates the possible existence of identity theft.
Service Provider - A third party engaged in performing an activity in connection with one or more covered accounts.

Detecting Red Flag Activity

1. Alerts, Notifications or Warning from a Consumer Reporting Agency
    a. A fraud or active duty alert is included with a consumer report.
    b. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
    c. A consumer reporting agency provides a notice of address discrepancy as defined in §41.82(b) of this part.
    d. 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:
        i. A recent significant increase in the volume of inquiries.
        ii. An unusual number of recently established credit relationships.
        iii. A material change in the use of credit, especially with respect to recently established credit relationships.
        iv. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
2. Suspicious Documents
    a. Documents appear to have been altered or forged.
    b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
    c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
    d. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
3. Suspicious Personally Identifiable Information (PII)
    a. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor.
        i. Examples: the address does not match any address in the consumer report; or the Social Security Number has not been issued, or is listed on the Social Security Administration's Death Master File.
    b. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer, e.g., there is a lack of correlation between the SSN range and the date of birth.
    c. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the institution.
        i. Examples: The address on an application is the same as the address provided on a fraudulent application; or the phone number on an application is the same as the number provided on a fraudulent application.
    d. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the institution.
        i. Examples: The address on an application is fictitious, a mail drop, or a prison; or the phone number is invalid, or is associated with a pager or answering service.
    e. The SSN provided is the same as that submitted by other persons opening an account or other customers.
    f. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.

g. The person opening the covered account or the person fails to provide all required personal identifying information on an application on in response to notification that the application is incomplete.
h. Personal identifying information provided is not consistent with personal information that is on file with the institution.
i. For financial institutions and creditors 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.
j. Unusual Use of, or Suspicious Activity Related to, the Covered Account.
k. Shortly, following the notice of a change of address for a covered account, the institution receives a request for new, additional, or replacement cards, or the addition of authorized users on the account.
l. The covered account is used in a manner commonly associated with known patterns of fraud.
    i. Example: The customer fails to make the first payment or makes an initial payment but no subsequent payments.
m. A covered account is used in a manner that is not consistent with established patterns of activity on the account.
    i. Examples: Nonpayment when there is no history of late or missed payments; a material increase in use of available credit; a material change in purchasing or spending patterns; a material change in electronic fund transfer patterns in connection with a deposit account; or a material change in telephone call patterns in connection with a phone account (can be cellular or landline).
n. 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).
o. Mail sent to customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
p. The institution is notified the customer is not receiving paper account statements
q. The institution is notified of unauthorized charges or transactions in connection with a customer's covered account.

4. 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 Institution

All Employees Procedures for the Rule

1. Access data in Lake Region State College's ConnectND system is restricted to those employees of the College with a need to know and for proper performance of their duties. These employees receive training related to FERPA and "Red Flag" regulations. Social Security numbers and Date of Birth are not used as authentication numbers and should be protected.
2. Every effort is made to limit the access to personal non-directory information to employees on campus with a legitimate need-to-know. Employees, who have been approved access to the administrative information databases, understand that they are restricted to using the information obtained only in the conduct of their job functions. The inappropriate use of such access and/or use of administrative data may result in disciplinary action up to, and including, dismissal from the University.
3. All paper files containing personal non-directory information are required to be in a secure location when not in use. All offices, when not occupied, are to be locked.

Student Administration Procedures for the Rule

1. Verify identification for any student, faculty, or staff requesting services. The identification should be scrutinized to verify that it has not been altered or forged.
2. Verify that the picture on the identification provided matches the appearance of the customer presenting the identification.
3. Verify that the information on the identification is consistent with other information on file at the college, particularly on the customer's account.
4. Do not share any more information with a customer than is documented in the student system if there is a full FERPA restriction on the account. If additional information is requested, the student should be forwarded to the Registrar's office for assistance.
5. Report to upper management without assisting the customer if the College ID provided is the same as that submitted by another customer.
6. Report to upper management if an account is used in a manner not consistent with regular patterns of activity, i.e. if a student receives more than one Short Term loan at a time, or over the period of one term.
7. Call or email the customer if mail addressed to the customer is returned as undeliverable although transactions continue to be conducted with their account.
8. Notify upper management if an account has three different address changes in the past ninety (90) days.
9. Investigate and verify the correctness of unauthorized charges or transactions assessed by Student Financial Services in connection with a customer's account. If there are questions regarding the correctness of departmental charges, refer them on to the appropriate department for resolution.
10. Notify upper management immediately if the College is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened, discovered, or manipulated a fraudulent account for a person engaged in identity theft.
11. Do not provide any information to an individual claiming to be the victim of identity theft without them providing evidence of a Police Case Number or an FTC affidavit of identity theft. If a customer needs assistance of this type, the request must be in writing with detailed information requested as well as proof of positive identification and proof of claim of identity theft (policy report or FTC affidavit).
12. Ensure that customers who call are not given information on an account if they cannot provide the College ID and customer name. Be cautious about callers who attempt to get financial information without providing any substantive knowledge about the account.
13. Employees and students are requested to report all changes in name, address, telephone or marital status to the Human Resources and Registration and Records offices as soon as possible; they should periodically verify those persons listed as contacts in case of an emergency, and those persons designated as beneficiaries to life and/or retirement policies.
14. A FERPA disclosure statement is sent out to students each year informing them of their rights under FERPA. The student is required to give written authorization to the Registrar's Office if their information is permitted to be shared with another party. The student is given the opportunity to provide billing addresses for third party billing.
15. Occasionally, the College will extend short term credit to a student for payment of their tuition bill or other items which thus creates a covered account. The student signs a short term promissory note, which is stored in a secured area.

Human Resources Policy and Procedures for the Rule

1. Staff who have access to HR and Payroll data have received training that non-directory information regarding employees is not to be provided unless approved in writing by the employee.
2. The College's official personnel files for all employees are retained in the Human Resources office in a locked file cabinet. Employees have the right to review the information contained in their personnel file.
3. Personnel records are classified as open records according to the North Dakota Century Code (Chapter 44-04).
4. Access data in Lake Region State College's ConnectND system is restricted to those employees of the College with a need to know and for proper performance of their duties. These employees receive training related to FERPA and "Red Flag" regulations.
5. Social Security numbers are not used as identification numbers and this data is classified as confidential.
6. Every effort is made to limit the access to confidential information to employees on campus with a legitimate need-to-know. Employees, who have been approved access to the administrative information databases, understand that they are restricted to using the information obtained only in the conduct of their job functions. The inappropriate use of such access and/or use of administrative data may result in disciplinary action up to, and including, dismissal from the University.

Oversight of Service Providers

The College remains responsible for compliance with the Red Flag Rules even if it outsources operations to a third party service provider. The written agreement between the College and the third party service provider shall require the third party to have reasonable policies and procedures designed to detect relevant Red Flags that may arise in the performance of their service provider's activities. The written agreement must also indicate whether the service provider is responsible for notifying only the College of the detection of a Red Flag or if the service provider is responsible for implementing appropriate steps to prevent or mitigated identify theft. Written agreements will be kept in the Administrative Affairs office.

Plan Responsibility, Review, Updates, and Approval

Responsibility for Lake Region State College's Identity Theft Prevention Program is assigned to the Information Security Response Team (see Information Security Response Policy).

These positions will work together and be responsible for coordinating Lake Region State College's Identity Theft Prevention Program including the following:

1. Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft and incorporate those red flags into the program;
2. Respond appropriately to any red flags that are detected to prevent and mitigate theft.
3. The Identity Theft Prevention Program will be reviewed and updated regularly by this team. Changes will be approved by the President of Lake Region State College.
4. Identify training and education relevant to the Identity Theft Prevention Program.
5. The Information Security Response Team will conduct an annual report on the compliance and effectiveness of the program and make recommendations for changes. The report should be filed with the President. Should an employee identify a "red flag" (patterns, practices and specific activities that signal possible identity theft), they are instructed to bring it to the attention of the Information Security Response Team. The team will investigate the threat of identity theft to determine if there has been a breach and will respond appropriately to prevent

future identity theft breaches. Additional actions may include notifying and cooperating with appropriate law enforcement and notifying the student or employee of the attempted fraud.

6. If there is a pattern, practice or activity relating to a university system-supported application, the Information Security Response Team will consult with the NDUS CIO or NDUS Security.

History

Administrative Council Approved 07/14/09

Administrative Council Approved 06/11/15