

## **North Dakota State University Identify Theft Prevention Program Plan**

### **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.

### **Definitions**

#### **Identity Theft:**

Fraud committed or attempted using the identifying information of another person without authority.

#### **Red Flag:**

A pattern, practice, or specific activity that indicates the possible risk of identity theft.

#### **Covered Account:**

A financial account whose purpose can be personal or business and is offered or maintained by NDSU . The account is designed to permit multiple payments or transactions. Covered accounts includes but is not limited to Bison Card accounts, credit/debit card processing, financial aid information, student loan information, business accounts, phone accounts, payroll account information; and any other account that NDSU offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of NDSU from identity theft, including financial operational, compliance, reputation, or litigation risks.

#### **Need to Know:**

Authorization is given to a user for whom access to the information must be necessary for the conduct of one's official duties and job functions as approved by the employee's supervisor.

#### **Confidential Data:**

Includes information that NDSU is under legal or contractual obligation to protect.

#### **Public Record:**

Defined as a record or data item that any entity either internal or external to NDSU can access.

### **Scope of Covered activities/ business processes, rules**

Any account or financial service that NDSU offers or maintains for which there is reasonably foreseeable risk to customers or to the safety and soundness of NDSU from identity theft, including financial operational, compliance, reputation, or litigation risks.

**Existing policies and practices****NDSU**

Policy 112 Pre-Employment and Current Employee Criminal Record Disclosure  
 Policy 120 Employee Information  
 Policy 158 Acceptable Use of Electronic Communications Devices;  
 Policy 509 Electronic Financial Transaction Policy;  
 Policy 513 Collection Policy;  
 Policy 600 Family Education Rights and Privacy Act of 1974 - FERPA and FERPA Notice;  
 Policy 703 Bison Card Terms and Conditions;  
 Policy 707 Card/Key Access and Building Security;  
 Policy 710 Computer and Electronic Communications Facilities;  
 Policy 713 Records Management;  
 Policy 718 Public/Open Records; NDSU Information Safeguarding (GLB); NDSU HIPPA  
 Policies/Procedures and Security Procedures

**NDUS**

Policy 511 Student Criminal History Background Checks and corresponding Procedure 511; Policy 602.3  
 Job Applicant/Employee Criminal History Background Checks and corresponding Procedure 602;  
 Policy 830.1 Student Payment Policy;  
 Policy 830.2 Refund Policy; Policy  
 1901.2 Computing Facilities and corresponding Procedure 1901.2;  
 Policy 1901.3 Information Technology Project Management and corresponding Procedure 1901.3;  
 Policy 1912 Public Records; Procedure 1912.1 Information Security Procedures; Procedure 1912.2  
 Student Records - Directory Information; Procedure 1912.3 Employee Personal Information

**Existing federal and state regulations**

The Federal Information Security Act of 2002 (FISMA)  
 The Family Education Rights and Privacy Act of 1974 (FERPA)  
 The Gramm Leach Bliley Act of 1999 (GLBA)  
 The Health Insurance Portability Accountability Act (HIPAA)  
 The Fair Credit Reporting Act  
 The Children's Online Privacy Protection Act  
 Fair and Accurate Credit Transaction Act of 2003 (FACTA)  
 Red Flag Rules – Interpretation of Sections 114 and 315 of FACTA  
 North Dakota Century Code, Chapter 44-04, Open Records  
 Payment Card Industry Data Security Standard (This is not a law, but is a set of standards for protecting  
 credit card information developed by the credit card industry.)

**Departments covered under the Red Flag Rule**

Any department that offers financial services.

**Red Flag Standards and Practices**

Many colleges, departments, and offices maintain files, both electronic and paper, of personal biographical, academic, health, financial, and admission records. These records may also include personal billing information, Perkins loans records, student institutional loans, and personal correspondence with employees, students, and parents. Policies to ensure compliance with Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act (FERPA), and Payment Card Industry security standards (PCI),

system and application security, and internal control procedures provide an environment where identity theft opportunities are mitigated. Personal financial records are safeguarded to ensure the privacy and confidentiality of student, parents, alumni, and employees.

The Office of Human Resources and Payroll performs criminal background checks on all potential employees prior to their date of hire.

NDSU is insured by a fidelity bond that covers losses arising from embezzlement, or the want of honesty, integrity, or fidelity by an employee or other person holding a position of trust.

- 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.
- The student is required to give written authorization to the Registration and Records office and/or the Bison Connection if their information is permitted to be shared with another party. A FERPA disclosure statement is distributed to students each year informing them of their rights under FERPA. The student is given the opportunity to provide billing addresses for third party billing.
- Occasionally, the University 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.
- Access data in NDSU's ConnectND system is restricted to those employees of the University 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 are not used as identification numbers and this data is classified as confidential.
- All paper files, when not in use, must be stored in locked filing cabinets. All offices must be secured during normal business hours and, when not occupied, are to be locked.
- Access to confidential employee data in NDSU's Human Resources and Payroll systems is restricted to only those employees who have a need to know and for proper execution of their job functions. These employees receive training related to FERPA and "Red Flag" regulations.
- Employees and students are requested to report all changes in name, address, telephone or marital status to the Office of Human Resources and Payroll and/or the Registration and Records office as soon as possible; they must periodically verify those persons listed as contacts in case of an emergency.
- The University ensures that all personal data (dates of birth, emplIDs, Social Security numbers, etc.) that it maintains in its personnel files and databases is protected. NDSU will not disclose personal information, except by written request or signed permission of the employee (e.g., the Campus Directory), or unless there is a legitimate business need-to-know, or if required by law.
- 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.

- The University's official personnel files for all staff are retained in the Office of Human Resources and Payroll. Official personnel files for faculty are maintained in the dean's office of the respective college.
- Any information classified as confidential contained within the personnel file remains confidential. Employees have the right to review the information contained in their personnel file.
- Personnel records are classified as open records according to the North Dakota Century Code (Ref: N.D.C.C. 44-04-18.1 (2)).

### **Detecting Red Flag Activity**

- Alerts, Notifications, or Warnings from a Consumer Reporting Agency
  - A fraud or active duty alert is included with a consumer report
  - A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report
  - A consumer reporting agency provides a notice of address discrepancy, as defined in §41.82(b) of the Final Rules for Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, as outlined in the 11/19/07 Federal Register
  - 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 recent 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
    - An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.
- Suspicious Documents
  - Documents appear to have been altered or forged
  - The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification
  - Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification
  - An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled
- Suspicious Personal Identifying Information
  - Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor.
    - 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
  - Personally identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the institution
  - 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
- 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.
  - 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
- The SSN provided is the same as that submitted by other persons opening an account or other customers
- 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
- The person having or opening a covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete
- Personal identifying information provided is not consistent with personal information that is on file with the institution
- 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.
- Unusual Use of, or Suspicious Activity Related to, the Covered Account
  - 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
  - The covered account is used in a manner commonly associated with known patterns of fraud.
    - Example: The customer fails to make the first payment or makes an initial payment but no subsequent payments
  - A covered account is used in a manner that is not consistent with established patterns of activity on the account.
    - 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)
  - 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)
  - Mail sent to customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account
  - The institution is notified the customer is not receiving paper account statements

- The institution 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 Institution

### **Responding to Red Flags**

- 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 their supervisor, who will bring it to the attention of the university registrar, Registration and Records; the associate VP of the Office of Human Resources and Payroll; the controller, accounting; the manager of Customer Account Services; the manager, Bison Connection; the director of Student Financial Services; or the director of the Student Loan Services Center. The administrator 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.

### **Oversight of Service Providers**

- Collection agency data sharing procedure
- Information service data sharing procedure (North Dakota Student Loan Center procedure for finding student whereabouts)

Section VI, part C, of the guidelines provides that, whenever a service provider is engaged to perform an activity in connection with one or more covered accounts, the institution should take steps to ensure 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. Thus, the guidelines make clear that a service provider that provides services to multiple financial institutions and creditors may do so in accordance with its own program to prevent identity theft, as long as the program meets the requirements of the regulations. The guidelines also provide an example of how a covered entity may comply with this provision. The guidelines state that a financial institution or creditor could require the service provider, by contract, to have policies and procedures to detect relevant red flags that may arise in the performance of the service provider's activities and either report the red flags to the financial institution or creditor or take appropriate steps to prevent or mitigate identity theft.

### **Plan Responsibility, Review, Updates, and Approval**

Responsibility for NDSU's Identity Theft Prevention Program is assigned to a team comprised of the following positions:

<u>Department</u>	<u>Position</u>
Division of Information Technology	NDSU Chief IT Security Officer (Co-Chair)
Accounting	Controller (Co-Chair)
Audit and Advisory Services	Internal Auditor
Customer Account Services	Manager, CAS

Bison Connection	Manager, Bison Connection
Office of the General Counsel	Legal Assistant
Student Financial Services	Director, SFS
Student Loan Service Center	Director, SLSC
Purchasing	Director, Purchasing
Human Resources	HR Administrator
Office of Registration and Records	Registrar

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

- 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;
- Detect red flags that have been incorporated into the program; and
- Respond appropriately to any red flags that are detected to prevent and mitigate theft.
- The Identity Theft Prevention Program will be reviewed and updated regularly by this team. Changes will be approved by the President of NDSU.
- Identify training and education relevant to the Identity Theft Prevention Program.
- Develop and review policies and procedures as appropriate to the Identity Theft Prevention Program.

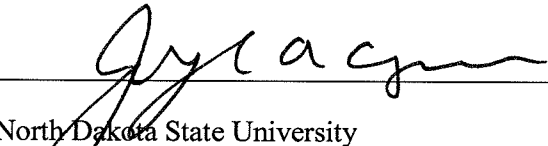
#### **Violations**

- The Federal Trade Commission is authorized to commence action in a federal district court in the event of a knowing violation of FACTA. Civil penalties for violations are capped at \$2,500 per offense. For universities that use and review consumer reports of customers, failure to comply with the address discrepancy regulations subjects violators to penalties not exceeding \$1,000.

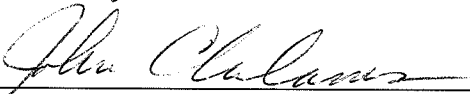
#### **Resource Links**

- Fair and Accurate Credit Transactions Act of 2003 (complete text): <http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf>
- Fair Credit Reporting Act: <http://www.ftc.gov/os/statutes/031224fcra.pdf>
- Federal Trade Commission: <http://www.ftc.gov>

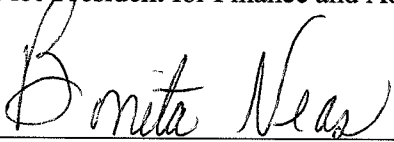
Approved

  
\_\_\_\_\_  
Date 4/27/09

President, North Dakota State University

  
\_\_\_\_\_  
Date 4/27/09

Vice President for Finance and Administration

  
\_\_\_\_\_  
Date 4-27-09

Vice President, Division of Information Technology