

# North Dakota State University Identity Theft Prevention Plan

## Background

This document outlines the required Red Flags Rule Program for North Dakota State University (NDSU).

The NDSU Identity Theft Prevention Program was developed and implemented to meet compliance with the Red Flags Rule and North Dakota University System Policy 802.7, Identity Theft. The Red Flags Rule was created by the Federal Trade Commission (FTC) along with other government agencies. The Red Flags Rule was based on section 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACTA). FACTA was put into place to help identity theft prevention and credit history restoration; improve use of and consumer access to credit information; enhance the accuracy of consumer report information; limit the use and sharing of medial information in the financial system; improve financial literacy and education; protect employee misconduct investigations; and improve relation to state laws.

The Red Flags Rule regulations require entities with accounts covered by the Red Flags Rule regulations, including universities, to develop and implement a written Identity Theft Prevention Program for combating identity theft in connection with certain accounts. The program must include reasonable policies (see Appendix A) and procedures for detecting, preventing and mitigating identity theft and enable the entity with covered accounts to:

1. Identify and detect red flags (relevant patterns, practices, and activities that could possibly signal identity theft);
2. Respond appropriately to any red flags that are detected and mitigate identity theft; and
3. Ensure the program is updated periodically to reflect changes in risks.

## 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

**Confidential Data:** Information that NDSU is under legal or contractual obligation to protect.

**Covered Account:** A financial account whose purpose can be personal or business and is offered or maintained by NDSU, 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.

**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, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;
2. Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;
3. Unique electronic identification number, address, or routing code; or
4. Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e)).  
16(16 CF.R. § 603.2(a)).

**Identity Theft:** A fraud committed or attempted using the identifying information of another person without authority. (16 CF.R. § 603.2(a)).

# North Dakota State University Identity Theft Prevention Plan

Need to Know: Authorization given to a user for whom access to the information must be necessary for the conduct of his/her official duties and job functions as approved by his/her supervisor.

Public Record: A record or data item that any entity either internal or external to NDSU can access.

Red Flag: A pattern, practice, or specific activity that indicates the possible risk of identity theft. See Appendix C for categories and examples of Red Flags.

## **Departments covered under the Red Flag Rule**

Any NDSU entity that maintains a covered account.

## **NDSU Red Flag Standards and Practices**

NDSU incorporates wording into policies and procedures to ensure compliance with the 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 to provide an environment where identity theft opportunities are mitigated. Financial records are safeguarded to ensure the privacy and confidentiality of students, parents, alumni, and employees. The NDSU standards and practices can be found in Appendix B.

## **Identifying Relevant Red Flags**

To identify relevant identity theft Red Flags, NDSU uses these risk factors for determination:

1. The types of accounts and types of data that is collected, stored and used;
2. The procedures and methods used to open or access the accounts and the data; and
3. Previous experience with identity theft.

## **Detecting Red Flags**

Current NDSU policies and procedures address the detection of Red Flags by:

1. Obtaining identifying information about, and verifying the identity of, a person opening a covered account; and
2. Authenticating customers, employees and students, monitoring transactions, and verifying the validity of change of address requests. Please see Appendix C, Red Flag Identification and Detection Grid.

## **Responding to Red Flags**

Staff members who identify a red flag will notify their supervisor who will, if needed, inform their administrator who will contact General Counsel for further advice and next steps, which may include:

- Monitoring a covered account for evidence of identity theft;
- Notifying the affected person(s);
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not sending a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

## **Preventing and Mitigating Identity Theft**

NDSU, based on the federal and state laws and other requirements such as PCI, has developed and implemented policies and procedures to prevent and mitigate identity theft. See Appendix A.

## **Oversight of Service Providers**

## North Dakota State University Identity Theft Prevention Plan

Examples of third party service providers include but are not limited to:

- Credit or banking institutions;
- Collection agency data sharing procedure;
- Information service data sharing procedure.

If and when third party service providers are used, NDSU can require them to have policies and procedures to detect relevant red flags that may arise in the performance of their activities and either report the red flags to NDSU or take appropriate steps to prevent or mitigate identity theft.

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

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

<b>Department</b>	<b>Position</b>
Accounting	Controller (Co-Chair)
Audit and Advisory Services	Internal Auditor, Manager, or designee
Bison Connection	Manager, Bison Connection, or designee
Customer Account Services	Director, CAS, or designee
Information Technology Division	NDSU Chief IT Security Officer (Co-Chair)
Office of the General Counsel	General Counsel, or designee
Office of Registration and Records	Registrar or designee
Purchasing	Director or designee
Student Financial Services	Director, SFS, or designee
Student Loan Services Center	Director, SLSC, or designee

These individuals will work together and be responsible for coordinating NDSU's Identity Theft Prevention Program including reviewing and updating the program to reflect changes in risks to customers or to the safety and security of the information provided to and created by NDSU. This will include but not be limited to:

- Identifying relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft, and incorporating those red flags into the program;
- Reviewing the Identity Theft Prevention Program and updating annually, which changes approved by the President of NDSU;
- Identifying training and education relevant to the Identity Theft Prevention Program;
- Developing and reviewing policies and procedures as appropriate to the Identity Theft Prevention Program.

The Red Flag Identity Theft plan will be approved and signed by the President of NDSU, the Vice President for Finance and Administration, and the Vice President for Information Technology.

### Resource Links

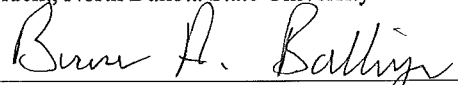
- Fair and Accurate Credit Transactions Act of 2003: [www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf](http://www.treasury.gov/offices/domestic-finance/financial-institution/cip/pdf/fact-act.pdf)
- Fair Credit Reporting Act: <http://www.ftc.gov/os/statutes/031224fcra.pdf>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

North Dakota State University  
Identity Theft Prevention Plan

Approved

  
\_\_\_\_\_  
Date 4-1-14

President, North Dakota State University

  
\_\_\_\_\_  
Date 4/1/2014

Vice President, Finance and Administration

  
\_\_\_\_\_  
Date 4/1/2014

Vice President, Information Technology

# North Dakota State University Identity Theft Prevention Plan

## North Dakota State University Appendix A

### State and Federal Laws; NDSU and NDUS Policies and Procedures Relevant to Red Flag Rules

#### 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 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  
Policy 602.3 Job Applicant/Employee Criminal History Background Checks and corresponding Procedure  
Policy 802.7 Identity Theft  
Policy 830.1 Student Payment Policy  
Policy 830.2 Refund Policy  
Policy 1901.2 Computing Facilities and corresponding Procedure  
Policy 1901.3 Information Technology Project Management and corresponding Procedure  
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  
North Dakota Century Code, Chapter 51-31, Identity Fraud  
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.)

# North Dakota State University Identity Theft Prevention Plan

## North Dakota State University Appendix B NDSU Red Flag Standards and Practices

NDSU incorporates wording into policies and procedures to ensure compliance with the 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, to provide an environment where identity theft opportunities are mitigated. Personal financial records are safeguarded to ensure the privacy and confidentiality of students, parents, alumni, and employees.

Current procedures and processes to protect an individual's identity include but are not limited to:

- Staff who have access to financial and confidential data receive training that non-directory information regarding employees is not to be provided unless approved in writing by the employee.
- Students are required to give written authorization to allow their confidential information to be shared with another party.
- Anytime a student signs a short term promissory note, it is stored in a secured area.
- Access to data in NDUS's ConnectND system is restricted to NDSU employees who have a need to know and for proper performance of their duties.
- Access to confidential data is restricted to only those employees who have a need to know and for proper execution of their job functions.
- 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.
- NDSU ensures that all confidential data it maintains in its files and databases is protected.
- Personnel records are classified as open records according the North Dakota Century Code (Ref: N.D.C.C. 44-04-18.1 (2)).

# North Dakota State University Identity Theft Prevention Plan

## North Dakota State University Appendix C Red Flag Identification and Detection Grid

This grid provides FTC categories and examples of potential red flags. Please note these examples are not exhaustive nor a mandatory checklist, but a way to help NDSU think through relevant red flags in the context of its business processes and procedures.

Red Flag	Detecting the Red Flag
<b>Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency</b>	
1. A fraud or active duty alert is included on a consumer credit report.	NDSU will verify that the fraud or active duty alert covers an applicant or customer and review the allegations in the alert.
2. A notice of credit freeze is given in response to a request for a consumer credit report.	NDSU will verify that the credit freeze covers an applicant or customer and review the freeze.
3. A notice of address or other discrepancy is provided by a consumer credit reporting agency.	NDSU will verify that the notice of address or other discrepancy covers an applicant or customer and review the address discrepancy.
4. A consumer credit report shows a pattern inconsistent with the person's history, such as a big increase in the volume of inquiries or use of credit, especially on new accounts; an unusual number of recently established credit relationships; or an account closed because of an abuse of account privileges.	NDSU will verify that the consumer credit report covers an applicant or customer, and review the degree of inconsistency with prior history.
<b>Category: Suspicious Documents</b>	
5. Identification presented looks altered or forged.	NDSU staff who work with customers will scrutinize identification presented in person to make sure it is not altered or forged.
6. The identification presenter does not look like the identification's photograph or physical description.	NDSU staff who work with customers will ensure that the photograph and the physical description on the identification match the person presenting it.
7. Information on the identification differs from what the identification presenter is saying.	NDSU staff who work with customers will ensure that the identification and the statements of the person presenting it are consistent.
8. Information on the identification does not match other information NDSU has on file for the presenter, like the original account application, signature card or a recent check.	NDSU staff who work with customers will ensure that the identification presented and other information on file matches and is consistent.
9. The application looks like it has been altered, forged, or torn up and reassembled.	NDSU staff will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled.
<b>Category: Suspicious Personal Identifying Information</b>	
10. Inconsistencies exist between the information presented and other things we know about the presenter or can find out by checking readily available external sources, such as the address does not match a consumer credit report, or the Social Security Number (SSN) has not been issued or is	NDSU staff will check personal identifying information presented to ensure that the SSN given has been issued but is not listed on the SSA's Master Death File. If NDSU staff receive a consumer credit report, they will check to see if the addresses on the application and the consumer report match.

## North Dakota State University Identity Theft Prevention Plan

listed on the Social Security Administration's (SSA's) Death Master File.	
11. Inconsistencies exist in the information that the customer provides, such as a date of birth that does not fall within the number range on the SSA's issuance tables.	NDSU staff will check personal identifying information presented to make sure that it is internally consistent by comparing the date of birth to see that it falls within the number range on the SSA's issuance tables.
12. Personal identifying information presented has been used on an account NDSU knows was fraudulent.	NDSU staff will compare the information presented with addresses and phone numbers on accounts or applications we found or were reported were fraudulent.
13. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.	NDSU staff will validate the information presented when opening an account.
14. The SSN presented was used by someone else opening an account or other customers.	NDSU staff will compare the SSNs presented to see if they were given by others opening accounts or other customers. Additionally, --
16. A person who omits required information on an application or other form does not provide it when told it is incomplete.	NDSU staff will track when applicants or customers have not responded to requests for required information and will follow up with the applicants or customers to determine why they have not responded.
17. Inconsistencies exist between what is presented and what NDSU has on file.	NDSU staff will verify key items from the data presented with the information on file.
18. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.	NDSU staff will authenticate identities for existing customers by asking challenge questions that have been prearranged with the customers, and for applicants or customers by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.
<b>Category: Suspicious Account Activity</b>	
19. Soon after NDSU receives a change of address request for an account, a request is received to add additional access means (such as debit cards or checks) or authorized users for the account.	NDSU will verify change of address requests by sending a notice of the change to both the new and old addresses so the customer will learn of any unauthorized changes and can notify NDSU.
20. A new account exhibits fraud patterns, such as where a first payment is not made or only the first payment is made, or the use of credit for cash advances and securities easily converted into cash.	NDSU will review new account activity to ensure that first and subsequent payments are made.
21. An account develops new patterns of activity, such as nonpayment inconsistent with prior history, a material increase in credit use, or a material change in spending or electronic fund transfers.	NDSU will review accounts to check for suspicious new patterns of activity such as nonpayment.
22. An account that is inactive for a long time is suddenly used again.	NDSU will review its accounts on at least a monthly basis to see if long inactive accounts become very active.
23. Mail NDSU sends to a customer is returned repeatedly as undeliverable even though the account	NDSU will note any returned mail for an account and take steps to verify the address if valid or if it has changed.



**North Dakota State University  
Identity Theft Prevention Plan**

remains active.	
24. NDSU learns that a customer is not getting his or her paper account or electronic statements.	NDSU will record on the account any report that the customer is not receiving paper and or electronic statements and immediately investigate the situation.
25. NDSU is notified that there are unauthorized charges or transactions to the account.	NDSU will verify if the notification is legitimate and involves a firm account and then investigate the report.
<b>Category: Notice From Other Sources</b>	
26. NDSU is told that an account has been opened or used fraudulently by a customer, an identity theft victim, or law enforcement.	NDSU will verify that the notification is legitimate and involves a firm account and then investigate the report.
27. NDSU learns that unauthorized access to the customer's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	NDSU will contact the customer to learn the details of the unauthorized access to determine if other steps are needed.

