PROCEDURES DOCUMENT

Identity Theft Prevention Program (ITPP)

under the FTC FACTA Red Flags Rule

FINANCE.UNCC.EDU/RESOURCES/MANUALS-GUIDES-PROCEDURES/RED-FLAGS-RULE

Contents

Purpose/Scope

The Fair and Accurate Credit Transactions Act (FACTA, Pub. L. 108-159) became federal law in 2003 as an amendment to the Fair Credit Reporting Act (FCRA). Sections 114 and 315 of FACTA directed the Federal Trade Commission (FTC), along with other banking agencies, to issue regulations regarding identity theft prevention, now known as the “Red Flags Rule” (“Rule,” see 16 CFR § 681). The Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program (“ITPP” or “Program”) designed to detect the warning signs (“red flags”) of identity theft in their daily operations. The purpose of this Program is to detect, prevent, and mitigate identity theft at the University.

ITPP Approval and Administration

The Board of Trustees of UNC Charlotte adopted an Identity Theft Prevention Program (ITPP) on April 16, 2009, which can be found on the Red Flags Rule web page. The University's Assistant Controller-Compliance in the Controller's Office is the designated Program Administrator and is responsible for the oversight, development, implementation, and administration of this ITPP.

Relationship to Other University Policies & Procedures

We have reviewed other policies, procedures and plans required by regulations regarding the protection of our customer information in the formulation of this ITPP, including University Policy 311, *Information Security,* and its supplemental regulations and procedures, and have attempted to establish this ITPP in a way that minimizes inconsistencies and duplicative efforts.

Relationship to GLBA, HIPAA, and FERPA: Note that the Red Flags Rule is not a data security regulation. Per the FTC's Red Flags Rule Overview, "Securing the data you collect and maintain about customers is important in reducing identity theft. The Red Flags Rule seeks to prevent identity theft, too, by ensuring that your business or organization is on the lookout for the signs that a crook is using someone else's information, typically to get products or services from you without paying for them. That's why it's important to use a one-two punch in the battle against identity theft: implement data security practices that make it harder for crooks to get access to the personal information they use to open or access accounts, and pay attention to the red flags that suggest that fraud may be afoot."[1] Thus, the Red Flags Rule *supplements* actual data security practices. The **Gramm-Leach-Bliley Act** (GLBA) should cover any policies and procedures dealing with the actual safeguarding of identity credentials to prevent their theft. University Supplemental Regulation 311.2 speaks to the GLBA and assigns the Information Technology Security Officer (ITSO) as the Program Officer with a committee of five campus representatives they may designate to oversee and coordinate certain Program elements. In the same manner, the **Health Insurance Portability and Accountability Act** of 1996 (HIPAA) requires safeguarding of Protected Health Information (PHI); the University's HIPAA compliance program is managed by the University's HIPAA Security Officer as described in University Policy 311.6. Finally, the **Family Educational Rights and Privacy Act** of 1974 (FERPA) requires safeguarding of education records; the University's FERPA compliance program is managed by the Office of Legal Affairs as described in University Policy 402.

The Red Flags Rule speaks to what happens if identity theft *is suspected* and the procedures necessary to mitigate any further exposure to the University and customer if identity theft *does* occur.

[1] An Overview, Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business

Key Definitions for Purposes of this Procedures Document

IDENTITY THEFT Any use or attempt by an individual to use another person's individual identifying information to obtain a thing of value, including money, credit, items, or services, such as medical care or education services to which the individual is not entitled.

RED FLAG A pattern, practices, or specific activity that indicates the possible existence of identity theft.

COVERED ACCOUNTS Accounts through which UNC Charlotte conducts financial activities that cause the University to be required to comply with the Red Flags Rule on an institution-wide basis.

PERSONALLY IDENTIFIABLE INFORMATION (PII) Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including, but not limited to: name; address; telephone number; social security number; date of birth; government-issued driver's license or identification number; passport number; taxpayer identification number; credit, debit, or banking account numbers; unique electronic identification number, including IP or other computer identifying address; unique biometric data such as fingerprint, voice print, retina or iris image or other unique physical representation.

KEY AREAS University Departments/units that are exposed to the risk of identity theft by the fact that they: 1) regularly and significantly rely on, and/or 2) have access to modify, PII.

Identifying Red Flags & Key Areas

To identify relevant identity theft Red Flags, we assessed these risk factors: 1) the types of covered accounts at the University, 2) other Key Areas that are exposed to the risk of identity theft (as defined in the Key Definitions section), and 3) previous experience with identity theft. There are 24 Key Areas identified by the Program Administrator at UNC Charlotte, as follows:

Key Area	Div	Reason included as Key Area
Enrollment Mgmt. – Office of Financial Aid	AA	Administers student emergency loans and loan accounts where UNC Charlotte is the creditor (constitute a Covered Accounts); handles financial aid PII
Enrollment Mgmt. – Office of the Registrar	AA	Logs and maintains the official academic record (which includes PII) for all students
Enrollment Mgmt. – Residency Determination Services	AA	Receipt, review, and maintenance of documentation w/PII for eligibility for exceptions to the NC residency requirements, which determines tuition charges
Enrollment Mgmt. – Undergraduate Admissions	AA	Processes Admissions PII
Graduate School	AA	Handles registrar services for grad students (academic petitions, graduation clearance, leaves of absence, etc.)
Graduate School, Admissions and Enrollment Management	AA	Receives, processes, handles, and stores all applications for admission materials for graduate applicants as well as international undergraduate applicants. Administers financial awards for grad students, incl. scholarships, financial aid, and assistantships.
Information Technology Services	AA	Manages system accesses and general information security
Office of International Programs	AA	Manages international student/faculty database
Office of the Provost – Academic Budget and Personnel (AABP)	AA	Handles faculty paperwork and imaging documents with PII
Auxiliary Services – 49er ID Card & Retail Services	BA	Administers 49er ID cards (constitutes a Covered Account); regularly handles cards w/PII
Auxiliary Services – Mail & Package Services	BA	Issues passports; handles U.S. mail
Auxiliary Services – Parking and Transportation Services	BA	Issues parking permits based on driver-related PII and handles other DMV-issued PII
Facilities Management – Motor Fleet	BA	Requires copy of driver's licenses to authorize use the of UNC Charlotte Motor Fleet Vehicles
Financial Services – eCommerce	BA	Manages PCI compliance
Financial Services – Office of the Bursar	BA	Handles Student Accounts PII; helps Financial Aid process student emergency loans and loan accounts where UNC Charlotte is the creditor (constitute a Covered Accounts)
Financial Services – Purchasing Card Program	BA	Handles employee PII; process p-card applications and p-card transactions
Financial Services – Tax & Payroll Office	BA	Handles tax and payroll information for the University

Financial Services – Vendor Relations	BA	Set up direct deposits for employees, students, and vendors
Human Resources – Employee Relations	BA	Administers employee loans up to $250 (constitutes a Covered Account)
Human Resources – Staff Employment and Records Mgmt.	BA	Handles faculty/staff paperwork and imaging documents w/PII (e.g., I-9s, background checks, and tax forms) and requests for related documentation
Police and Public Safety	BA	Manages criminal incident database; responds to incidents where fraud is suspected
Dean of Students Office, Office of Student Conduct	SA	Manages student conduct process and records
Housing and Residence Life	SA	Handles Housing-related PII (students are mainly directed to My UNC Charlotte to make changes)
Student Health Center	SA	Handles Protected Health information governed by HIPAA

In addition, we considered Red Flags from the following five categories from Supplement A to Appendix A of the FTC's Red Flags Rule, as they fit our situation: 1) alerts, notifications or warnings from a credit reporting agency; 2) suspicious documents; 3) suspicious personal identifying information; 4) suspicious account activity; and 5) notices from other sources. We understand that some of these categories and examples may not be relevant to the University, and some may be relevant only when combined or considered with other indicators of identity theft. We also understand that the examples are not exhaustive or a mandatory checklist but a way to help our employees think through relevant red flags in the context of our operations. Based on a review of the risk factors, sources, and FTC examples of Red Flags, we have identified our University's Red Flags, as listed in the first column ("Red Flag") of the *Red Flag Identification and Detection Grid* section.

Red Flag Identification and Detection Grid

Note that these procedures are included here for basic guidance. You may develop more detailed procedures for your area as necessary. In general, the following should be done in all situations where Red Flags are suspected:

- Once potentially fraudulent activity is detected, an employee must act quickly as an appropriate rapid response can protect individuals and the University from damages and loss. At a minimum, the employee must notify their supervisor, gather all related documentation, and complete the Red Flag Detection Form, which is sent to the Red Flags Rule Program Administrator.
- Additional investigation of authenticating information will be conducted to determine whether the attempted transaction was fraudulent or authentic.
- Take appropriate actions immediately if a transaction is determined to be fraudulent. Actions may include:
    - Canceling the transaction;
    - Notifying and cooperating with appropriate law enforcement;
    - Determining the extent of liability of the University; and
    - Notifying the actual individual upon whom fraud has been attempted.

Red Flag	Detecting the Red Flag
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency	
1. Notice/report of fraud or active duty alert	• Verify activity reported with applicant/ customer. • If verified, review the notice, freeze, or degree of inconsistency with prior history, and proceed with the evaluation of the applicant based on a consumer report received. • If unable to verify, do not use this report in evaluating an applicant – no further action required.
2. Notice/report of a credit freeze on an applicant	
3. Indication of activity that is inconsistent with an applicant's usual pattern or activity history Examples: a large 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.	
4. Notice of address or another discrepancy	• Compare the reported address (or other information) with that provided by the applicant and, if necessary, contact the applicant to verify. • If the address (or other information) has been verified, report it to the credit report agency. • If unable to determine the relationship between the applicant and the notice, do not use the report to evaluate the applicant and notify the applicant. No further action required. *Also, see the FTC's Address Discrepancy Rule (16 CFR part 641.1).*
Category: Suspicious Documents	
5. Identification presented looks altered, forged, or inauthentic.	• Retain and scrutinize identification or other document presented to ensure: o it is not altered, forged, or torn up and reassembled; o that the photograph and the physical description on the identification match the person presenting it; o that the identification and the statements of the person presenting it are consistent; and/or o that the identification presented and other information we have on file is consistent. • Notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
6. The person presenting identification does not look like the identification's photograph or physical description.	
7. The person presenting identification conveys information that differs from what is indicated on the identification.	
8. Information on the identification does not match other information on file for the customer (e.g., employee/student information in Banner).	
9. A request for information, application, or other document looks like it has been altered, forged, or torn up and reassembled.	
Category: Suspicious Personal Identifying Information	
10. Identifying information is inconsistent with other external information sources. Examples: an address that does not match the address printed on an FAFSA form, a Social	• Inspect information and compare with other external information sources. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven.

Security Number (SSN) that has not been issued or is listed on the Social Security Administration's (SSA's) Master Death File.	• If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
11. Identifying information is inconsistent with other information provided by the customer Examples: inconsistent dates of birth, SSNs, or addresses on two forms received.	• Inspect information and ask the customer to validate which information is accurate. • Retain information and notify management for assistance if necessary. Do not provide services until correct identifying information is proven. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
12. Identifying information is associated with known fraudulent activity. Example: an address or phone number being used is also known to be associated with a fraudulent application.	• Inspect information and compare with documentation indicating fraudulent activity. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
13. Identifying information suggests fraud or is of the type commonly associated with fraudulent activity. Examples: an address that is obviously fictitious, an address that is a mail drop or a prison, a phone number is invalid.	• Inspect information and determine its validity. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
14. The SSN or UNC Charlotte ID number is the same as that submitted by another customer.	• Inspect information and request to see the student's Social Security card, 49er Card, or driver's license. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • Place hold on the original customer who provided the duplicate ID number if identity is proven. Direct customer to the FTC Identity Theft website if necessary to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
15. Address or phone number is the same as that presented by an unusually large number of other customers.	• Request and inspect information to determine its validity. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
16. A customer omits required personal identifying information on an application or other form or does not provide it in response to notification that the application/form is incomplete.	• Do not provide services or award aid until application/form is complete. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
17. Identifying information is inconsistent with internal information sources on file.	• Inspect information and compare with information in Banner or other official University systems of record or data files. • Retain information and notify management for assistance if necessary. Do not provide services until identity is proven. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form

18. A person seeking access to systems or sensitive information cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question. Example: Staff member cannot answer security challenge question required to regain access to eCommerce systems.	• Do not provide services, reset passwords, or otherwise provide access until identity is proven. • Follow any protocols established to recover access to the system in question (e.g., by notifying the system administrator to send a password reset link to the person's email). • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
Category: Suspicious Account Activity	
19. Change of address request followed shortly by request for a name change.	• Request official documentation reflecting name change (court order, marriage certificate, etc.) and compare with photo identification. • Verify change of address previously submitted. • If the customer did not initiate the action(s) and identity theft of the customer's information is suspected, direct customer to FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
20. An account is used in a manner inconsistent with established patterns of activity on that account. For example, payments are no longer made on an otherwise consistently up-to-date account.	• Banner automatically places a financial hold on overdue accounts and restricts certain services from being provided until the Bursar's Office has removed the hold. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
21. Mail sent to a customer is repeatedly returned as undeliverable even though the account remains active.	• Attempt to contact the customer via the contact information on file. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
22. Customer notifies UNC Charlotte (via phone, email, or in-person) that the customer is not receiving mail.	• Verify address information with the customer and ensure listed addresses are active. • If the address on file was not entered by the customer, notify management for assistance. If identity theft of the customer's information is suspected, direct the customer to FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
23. Customer notifies UNC Charlotte (via phone, email, or in-person) that an account with the University has unauthorized activity.	• Verify if the notification is legitimate and involves a UNC Charlotte account. Notify management for assistance to investigate the activity. • If a customer's account does have unauthorized activity and identity theft of the customer's information is suspected, direct the customer to FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form

24. Customer notifies UNC Charlotte (via phone, email, or in-person) that unauthorized access to a University account that uses NinerNET authentication (email, My UNC Charlotte, Canvas, 49er Mart, etc.) has occurred. Example: Customer is automatically logged off during an online session due to multiple login attempts from an external site.	• Verify if the notification is legitimate and involves a UNC Charlotte account. Notify management for assistance to investigate the activity. • Instruct the customer to reset the account password immediately. • If unauthorized access did occur and identity theft of the customer's information is suspected, direct the customer to FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form
Category: Notice From Other Sources	
25. A customer, identity theft victim, or law enforcement agent notifies UNC Charlotte (via phone, email, or in-person) that an account has been opened or used fraudulently.	• Verify if the notification is legitimate and involves a UNC Charlotte account. Notify management for assistance to investigate the activity and determine if any actions are needed (e.g., inactivating direct deposit, placing a financial hold on the account). • Direct customer to FTC Identity Theft website to learn what steps to take to recover from identity theft, if the customer has not already done so. • If the fraud occurred during the conduct of University business, report the incident to Campus Police and complete the Red Flag Detection Form.
26. We learn 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.	• Verify if the notification is legitimate and involves a UNC Charlotte account. Notify management for assistance to investigate the activity and determine if any actions are needed (e.g., inactivating direct deposit, placing a financial hold on the account). Also, see University Policy 311.5, *Personal Information Security Breach Notification Procedures.* • If identity theft of customer's information is suspected, direct customer to FTC Identity Theft website to learn what steps to take to recover from identity theft. • If fraud is reasonably suspected, report to Campus Police and complete the Red Flag Detection Form

Preventing and Mitigating Identity Theft

PROCEDURES TO PREVENT IDENTITY THEFT

Student Enrollment
To prevent identity theft associated with the enrollment of a student, University personnel shall take the following steps to obtain and verify the identity of the person opening the account:

- Require certain Identifying Information such as name, date of birth, academic records, home address or other identification; and
- Verify the individual's identity at the time of issuance of individual identification card (review of driver's license or other government-issued photo identification).

Existing Accounts
To prevent identity theft for an existing Covered Account, University personnel shall take the following steps to monitor transactions on an account:

- Verify the identification of individuals if they request information (in person, via telephone, via facsimile, via email);
- Verify the validity of requests to change billing addresses by mail or email and provide the individual a reasonable means of promptly reporting incorrect billing address changes; and
- Verify changes in banking information given for billing and payment purposes.

Consumer ("Credit") Report Requests
To prevent identity theft regarding an employment or volunteer position for which a credit or background report is sought, University personnel shall take the following steps to assist in identifying address discrepancies:

- Require written verification from any applicant that the address provided by the applicant is accurate at the time the request for the credit report is made to the consumer reporting agency; and
- If notice of an address discrepancy is received, verify that the credit report pertains to the applicant for whom the requested report was made and report to the consumer reporting agency an address for the applicant that the University has reasonably confirmed is accurate.

Protection of Identifying Information
To further prevent the likelihood of Identity Theft occurring during the conduct of University business, the University will take the following steps with respect to its internal operating procedures to protect PII:

- Ensure that its website is secure or provide clear notice that the website is not secure;
- Ensure complete and secure destruction of paper documents and computer files containing individual account information when a decision has been made to no longer maintain such information;
- Ensure that office computers with access to PII are password protected;
- Ensure that laptops are password protected and encrypted;
- Avoid use of social security numbers when possible;
- Ensure the security of physical facilities that contain PII;
- Ensure that transmission of PII is limited and encrypted when necessary;
- Ensure computer virus protection is up to date; and
- Require and keep only the kinds of individual information that are necessary for University purposes.

Hard Copy Distribution
Each employee and contractor performing work for the University will comply with the following security measures related to hard copy files with PII:

- File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with PII will be locked when not in use, when unsupervised, and at the end of each workday.

- Clear desks, workstations, work areas, printers and fax machines, and common shared work areas of all documents containing PII when not in use.
- Whiteboards, dry-erase boards, writing tablets, and other writing surfaces in common shared work areas with PII will be erased, removed, or shredded when not in use.
- When documents containing PII are discarded, they will be placed inside a locked shred bin or immediately shredded using a mechanical crosscut or Department of Defense-approved shredding device. Label locked shred bins as “Confidential paper shredding and recycling.”

PROCEDURES TO MITIGATE IDENTITY THEFT

If University personnel are notified of a Red Flag or our detection procedures show evidence of a Red Flag, such personnel should take the steps outlined below, as appropriate to the type and seriousness of the threat:

- Watch. We will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
- Check with the customer. We will contact the customer, describe what we have found, and verify with them that there has been an attempt at identity theft.
- Change passwords. We will change any passwords or other security measures that permit access to the affected account(s).
- Deny new accounts. If we find that the applicant is using an identity other than his or her own, we will deny opening any new accounts.
- Provide new identification. If a customer’s identification number has been compromised, we will provide the individual with a new UNC Charlotte ID number.
- Implement two-factor identification. If not already in place, look at implementing multi-factor authentication to help prevent unauthorized access to accounts and systems.
- Heightened risk. We will determine if a particular reason exists that has made it easier for an intruder to seek access, such as a customer’s lost wallet, mail theft, a data security incident, or the occurrence of a customer giving his or her account information to an imposter pretending to represent the University or to a fraudulent website.
- Check similar accounts. We will review similar accounts the customer has with the University to see if other attempts to access them without authorization have been made.
- Collect incident information. Personnel will complete a Red Flag Detection Form, which is sent to the Red Flags Rule Program Administrator.
- Report. If we find that the applicant is using an identity other than his or her own, we will report it to Police & Public Safety (704-687-2200), who may determine if it is subsequently necessary to notify other federal or state agencies if organized or widespread crime is suspected or, if mail is involved, the US Postal Inspector.

Service Providers

In the event the University engages a Service Provider to perform an activity in connection with one or more of its Covered Accounts, the University will take the following steps to ensure the Service Provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of Identity Theft:

- Require, by signed contract, that Service Providers have such policies and procedures in place; and
- Require, by signed contract, that Service Providers review the University's Program and report any Red Flags to the Program Administrator.

Program Administration

The Program Administrator, currently the Assistant Controller-Compliance in the Controller's Office, is responsible for developing, implementing, and administering the University's ITPP. Appropriate staff shall report to the Program Administrator at least annually on compliance by the University with this Program. The report shall address matters such as the effectiveness of the policies and procedures of the University in addressing the risk of Identity Theft in connection with the opening of Covered Accounts and with respect to existing Covered Accounts; Service Provider arrangements; significant incidents involving Identity Theft and the University's response; and recommendations for material changes to the Program.

Key Resources

University Red Flags Rule Pages

OVERVIEW	http://finance.uncc.edu/resources/manuals-guides-procedures/red-flags-rule
ANNUAL SURVEY	https://webforms.uncc.edu/financeunccedu/red-flags-rule-annual-survey
RED FLAG DETECTION FORM	https://webforms.uncc.edu/financeunccedu/red-flag-detection-form

FTC Resources

FTC DATA SECURITY RESOURCES	http://business.ftc.gov/privacy-and-security/data-security
FIGHTING IDENTITY THEFT WITH RFR HOW TO GUIDE FOR BUSINESS	http://business.ftc.gov/documents/bus23-fighting-identity-theft-red-flags-rule-how-guide-business
FTC CONSUMER INFORMATION IDENTITY THEFT	http://www.consumer.ftc.gov/features/feature-0014-identity-theft

University Policies

OFFICE OF LEGAL AFFAIRS	https://legal.uncc.edu/policies/university-policies

Acronyms

CFR	Code of Federal Regulations
CISO	Chief Information Security Officer
FACTA	Fair and Accurate Credit Transactions Act
FAFSA	Free Application for Federal Student Aid
FCRA	Fair Credit and Reporting Act
FERPA	Family Educational Rights and Privacy Act of 1974
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act
HIPAA	Health Insurance Portability and Accountability Act of 1996
ITPP	Identity Theft Prevention Program
ITS	Information Technology Services department
NCRA	Nationwide Consumer Reporting Agency (Experian, Equifax, TransUnion)
PHI	Protected Health Information
PII	Personally Identifiable Information
SSA	Social Security Administration
SSN	Social Security Number

Document History and Annual Review

These Procedures were constructed using various resources, including the University's ITPP, the *FTC FACT Act Red Flags Rule Template,* and The University of Texas at San Antonio's Red Flags Rule policy. The following departments contributed to the creation and review of this document: Financial Services, the Office of Legal Affairs, the Internal Audit Department, ITS Information Systems, and the Division of Institutional Integrity's Ethics and Compliance Office. We gratefully acknowledge the contributions and collaboration of the staff within these.

Creation date: June 2013
Our identity theft policies, procedures, and internal controls will be reviewed and updated periodically to ensure they account for changes both in regulations and in our operations.

Revision dates: March 2014 (updated links); April 2014 (updated Key Areas); June 2015 (updated Key Areas & links); October 2015 (updated 49er Express text to My UNC Charlotte); June 2016 (added Accounts Payable, Purchasing Card, and Payroll to Key Areas); June 2017 (updated key areas); June 2018 (updated key areas and web links); June 2019 (updated key areas, links, policy reference and minor related content changes); June 2020 (link and minor clarification updates);