BYU

BRIGHAM YOUNG

UNIVERSITY

Provo, Utah

Fair and Accurate Credit Transaction Act
Identity Theft Compliance Program

Table of Contents

1.0 OVERVIEW

The Fair and Accurate Credit Transactions Act (FACTA) of 2003, an amendment to the Fair Credit Reporting Act (FCRA), was created for the purpose of implementing requirements for financial institutions and creditors to develop and implement written identity theft prevention programs. The Federal Trade Commission (FTC), the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations implementing sections 114 and 315 of FACTA, referred to as the Red Flag Rules. Brigham Young University (BYU) meets the definition established by FACTA as a "creditor" and is therefore required to comply with the Red Flag Rules. Under the Red Flag Rules, financial institutions and creditors must develop a written program that identifies and detects the relevant warning signs – or "red flags" – of identity theft. These may include unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Board of Directors or senior employees of the financial institution or creditor, include appropriate staff training, and provide for oversight of any service providers.

2.0 POLICY STATEMENT

Security over information maintained by BYU is of prime importance both to BYU and to the persons about whom we maintain information. Sensitive information held by BYU includes:

- Credit card holder information (name, card number, PIN numbers)
- Personally identifiable information (name, social security number, birth date, etc.)
- Student information (grades, class standing, course progress)
- Employee information (name, social security number, bank account number, etc.)

While the university cannot guarantee the security of this information, it is our goal to provide reasonable protection for sensitive information maintained by BYU and to comply with both state and federal information security and privacy laws and regulations.

3.0 STATUTES & REGULATIONS

- ▷ 16 CFR Part 681
- ▷ Appendix A to Part 681—Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation
- ▷ 15 U.S.C. 1681s(a)(1)
- ▷ 31 U.S.C 5318(l) (31 CFR 103.121)

4.0 PURPOSE & SCOPE

This compliance program provides a description of the university's program to comply with the requirements of FACTA.

BYU's Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts includes the following objectives for identifying, detecting, responding, and ensuring the Program is appropriate and in compliance with all statutes and guidelines.

4.1 **Identify:** Identify relevant patterns, practices, and specific forms of activity that are Red Flags signaling possible identity theft.

4.2 **Detect:** Detect instances of Red Flags that have been incorporated into the Program using suggested federal guidelines including applicable portions of the "Customer Identification Programs" 31 U.S.C 5318(l) (31 CFR 103.121). The responsibility to detect Red Flags shall also extend to any service providers under contract with BYU.

4.3 **Respond:** Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft. BYU shall begin to respond immediately upon the detection of a Red Flag and continue to respond until the validity of an account and related charges are satisfactorily verified.

4.4 Ensure the Program is updated periodically: The Program, including the identification of new Red Flags, should be updated periodically to be relevant, to reflect changes in risks to customers, or to the safety and soundness of BYU from identity theft. Factors to consider include the following:

- The experiences of BYU with identity theft;
- Changes in the methods of identity theft;
- Changes in methods to detect, prevent, and mitigate identity theft;
- Changes in the types of accounts that BYU offers or maintains; and
- Changes in the business arrangements of BYU including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.

5.0 PROCEDURES

The FTC has issued general rules and guidelines for complying with the referenced statutes and regulations. Detailed procedures, guided by the general FTC rules and guidelines, implementing this Program at BYU are included as Appendix A and are maintained by Financial Services. The detailed procedures will be made available to all departments with FACTA compliance responsibilities through the use of a BYU web site.

6.0 RESPONSIBILITIES

Executive Risk Management and Compliance Committee (ERMCC) is responsible for BYU's compliance with FACTA and for designating a FACTA Compliance Coordinator. The ERMCC is the designated committee responsible for:

1. Assigning specific responsibility for the Program's implementation;
2. Reviewing reports prepared by staff regarding compliance; and
3. Approving material changes to the Program as necessary to address changing identity theft risks.

FACTA Compliance Coordinator is responsible to:

1. Develop BYU's FACTA Compliance Program to achieve the purposes of the program as defined above,
2. Coordinate the development of policies and procedures to help achieve compliance with the associated statutes and regulations,
3. Train all departments with FACTA compliance responsibilities,
4. Provide an annual report to the ERMCC on BYU's compliance with the detection, prevention, and mitigation elements of the law (16 CFR 681.2),
5. Periodically conduct and update a risk assessment to identify accounts covered by the law, how the accounts are protected from identity theft, and maintain communication with department managers having FACTA compliance responsibilities.
6. Stay current regarding changes to the law and best practices regarding FACTA compliance.

Department Managers with FACTA compliance responsibilities are responsible to regularly review current practices and to oversee the initial training of new employees as well as to communicate any instances of concern or known infractions FACTA's Red Flag Rules to the BYU's FACTA Compliance Coordinator.

7.0 TRAINING/COMMUNICATION REQUIREMENTS

Training of all departments will be administered and monitored by the FACTA Compliance Coordinator. This includes regular reviews of procedures by department personnel concerning compliance with and reporting of Red Flag Rules policies and procedures. Reports will be provided concerning any need for modification to currently adopted policies as well as any occurrences of identity theft activity which have required procedures to change. Updated instructional material disbursed by regulatory agencies or industry associations will also be included and implemented where necessary. Training programs will incorporate

input from departments with FACTA compliance responsibilities. BYU may also develop certification programs as appropriate.

8.0 MONITORING REQUIREMENTS & REPORTS

8.1 **Monitoring:** At least annually, the FACTA Compliance Coordinator will meet with the department managers with FACTA compliance responsibility and review their FACTA compliance program, including their procedures for identifying, detecting, and responding to the Red Flags as defined in BYU's procedures. The results of these reviews will be included in the annual report to the ERMCC.

8.2 **Reporting:** The FACTA Compliance Coordinator shall immediately inform the ERMCC of any significant identity theft or Red Flags which indicate a potential security problem requiring immediate mitigating action. Additionally, the FACTA Compliance Coordinator shall provide to the ERMCC an annual report on compliance with the Program including items such as:

- An assessment of the current effectiveness of the program in detecting Red Flags and reducing the opportunity for, and impact of identity theft
- BYU responses to the observance of Red Flags
- Training programs conducted
- Review of service provider compliance with Red Flag rules
- Recommended material changes in the Program

.

APPENDIX A

FACTA Identity Theft Compliance Program - Procedures:

A. General Guidelines

The following procedures provide specific guidance regarding actions that should be taken to comply with the FACTA Identity Theft Compliance Program, frequently referred to as the "Red Flags" rules. The sections dealing with the administration of the program provide instructions regarding specific tasks that will be performed under the direction of the FACTA Compliance Coordinator. These tasks ensure that BYU employees are properly trained, that the program is appropriately updated for changes in circumstances, and that all relevant issues are reported to the Executive Risk Management and Compliance Committee (ERMCC).

Guidance is also provided in these procedures to assist individual employees who are either users or providers of personal information. While numerous procedures could be developed, the specific procedures identified herein represent the "minimum standard" that BYU employees should follow. If an employee has any reason to believe that a problem has not been adequately resolved through use of these procedures he/she should contact the FACTA Compliance Coordinator for assistance in using additional procedures.

B. Applicability

These procedures are applicable to all BYU departments and employees. Generally, employees who perform one or more of the following tasks need to be especially aware of these procedures.

Employees who:

- Use credit reports for credit granting decisions
- Provide credit reporting information to 3rd parties
- Maintain (set-up or modify) personal information such as name, address, Social Security #, BYU ID, Department charge account #, etc… for any BYU student, customer or employee
- Provide account information to students or customers such as balances, transaction or payment information, etc…

The following campus departments have been identified as primary users, providers, or maintainers of such information, and accordingly will be the focus of initial training and be included in routine reporting.

Department	Type of Information or Usage
Student Financial Services	• Access to and ability to modify address & other personal info • Obtain and use credit reports • Provide credit reporting info to credit agencies • Respond to account queries
Student Services	• Access to and ability to modify address & other personal info • Accept payments on account • Respond to account queries
Registrar	• Access to and ability to modify address & other personal info
International Student's Office	• Access to and ability to modify address & other personal info
Student Auxiliary Services	• Access to and ability to modify address & other personal info
Alumni Office	• Access to and ability to modify address & other personal info • Accept payments on account
BYU Bookstore	• Use of credit reports • Manage credit card program (Bookstore Card)
Signature Card Office	• Access to and ability to modify address & other personal info
Treasury Services	• Access to and ability to modify address & other personal info
OIT	• Access to and ability to modify address & other personal info

Traffic Office	• Access to and ability to modify address & other personal info • Establish covered accounts – non students • Respond to account queries
Division of Continuing Education (including Independent Study)	• Access to and ability to modify address & other personal info • Use of credit reports • Accept payments on account • Respond to account queries
Daily Universe	• Establish covered accounts • Obtain and use credit reports • Respond to account queries
Special Events	• Establish covered accounts
Performing Arts Management	• Establish covered accounts • Respond to account queries • Accept payments on account
Student Auxiliary Services	• Establish covered accounts • Respond to account queries • Accept payments on account

C. Definitions – The following definitions have been adapted from Federal regulations and other authoritative sources to meet BYU's unique circumstances.

C.1 Challenge Questions – Questions used to verify the identity of a student or customer who inquires about an account by phone or email. Answers to these questions should be readily known by the actual student or customer but would not be readily apparent from the contents of a stolen wallet or account statement.

C.2 Covered Accounts - An account that BYU offers or maintains:

1.) Primarily for personal, purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, student loan, tuition, housing or other payments; and

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

C.3 Customer – Students, Faculty/Staff, and any other entity conducting business with BYU.

C.4 Customer Identification Programs – Federally mandated procedures for preventing identity theft identified in 31 U.S.C 5318(l) (31 CFR 103.121**)**

C.5 FACTA – Fair and Accurate Credit Transactions Act

C.6 Personal Information – Pieces of information which individually or collectively can be used to identify an individual and gain access to financial or other private information. Such information includes but is not limited to:

1.) Name
2.) Social Security Number
3.) Student Identification
4.) Birth Date
5.) Address

C.7 Red Flags – Any pattern of activity, practice, notice, warning or suspicious incident which indicates the *possibility* of identity theft or an attempt to gain unauthorized access to personal information.

D. Detecting, Preventing and Responding to Identity Theft

To comply with Red Flags rules, BYU will use the following procedures to detect, prevent, and respond to potential inquires that might result from identify theft. These procedures will be applied to all covered accounts provided by BYU. The procedures also identify the methods that BYU uses to open new covered accounts.

D.1 Identified Red Flags

Situations, notices, or procedures that constitute Red Flags include, but are not limited, to the following:

1.) Alerts, notifications, or warnings from a consumer reporting agency. A credit report may indicate a credit freeze or unusual patterns of activity such as:

   a) Significant numbers of recent inquiries by creditors

   b) Sudden changes in use of credit

   c) Recent charges up to the limit allowed on credit cards

2.) Notices from customers, victims of identity theft, law enforcement authorities, or other entities about possible identity theft in connection with covered accounts.

3.) Suspicious personal identifying information. This can include changes or differences in personal identifying information when compared to already existing BYU data, such as:

   a) A variation in the SSN provided by the customer

   b) Variations in address or phone number information

4.) Suspicious documents, including:

   a) Documents that appear to be altered or forged

   b) Documents that are not consistent with already verified information known to BYU. This includes any personal identification information not consistent with readily accessible information that is on file with BYU, such as a signature card or recent check.

5.) Suspicious activity relating to a covered account. This could include:

   a) Incorrect or unanticipated answers to Challenge Questions.

   b) Account inquiries from seemingly unrelated individuals or third parties.

D.2 Detecting Red Flags Procedures

BYU personnel will take the following steps to detect Red Flags when monitoring transactions on covered accounts:

1) The preferred method for making changes to an existing student's demographic information is by the student through the secure, online website. Use of the online website will generally be considered safe and no additional procedures will be used unless BYU receives other information indicating potentially fraudulent activity.

2) Consumer reporting agencies may receive bad or conflicting information from a number of sources; agencies may also report addresses discrepancies provided by BYU to the agency as discrepancies when compared with their information. Therefore, information included in alerts, notifications or warnings from a consumer reporting agency should be verified prior to making changes to student or customer information recorded in BYU systems. Specific actions, which the department or individual receiving the notice should use to verify such information include:

    a) Address Discrepancies in Consumer Credit Reports

        i. When BYU obtains a consumer report and is notified there is an address discrepancy:

            a) Compare the address information in the consumer report with the application or other information BYU has on file.

            b) If an address used to obtain a consumer report was obtained from a third party source, then BYU will verify the information in the consumer report with the student or customer.

        ii. When BYU is notified by a consumer reporting agency that an address supplied by BYU is different than that currently on file with the consumer reporting agency:

            a) Verify the address with the student or customer

b) Review BYU's own records to verify the address of the student or customer

c) Verify the address through third-party sources

b) Address changes relating to the issuance of credit cards

Special care must be given to address change requests when BYU issues credit cards. If BYU receives a request for a change in address for cardholder, and subsequently, within a relatively short period of time (typically 30 days), receives a request for a replacement or additional card, the request will be considered suspicious. Under these circumstances BYU may not issue an additional or replacement card until the following steps are completed:

i. Assess the validity of the change of address by procedures described above in section D.2 2); or

ii. Notify the cardholder of the request

a) At the cardholder's former address; or

b) By any other means of communication that BYU and the cardholder have previously agreed to use; and

c) Provide to the cardholder a reasonable means of promptly reporting the propriety of the address change and the need for an additional or replacement card

c) Notice of changes in credit patterns

When BYU receives any notice that a student or customer is experiencing significant changes in credit, such as a credit freeze, significant increases in the number of credit inquiries, sudden changes in the use of credit, or recent charges that run credit limits to their maximum, the mitigating responses identified in section D.3 should be followed.

d) Direct Dispute about information reported to consumer reporting agencies

When a consumer notifies BYU of a dispute relative to information provided to consumer reporting agencies, BYU will investigate the dispute, independent of any other notice from a consumer reporting

agency, as required by section 611 (a) (1) of the Fair Credit Reporting Act.

3.) Notices from students, customers, other victims of identity theft, law enforcement authorities, or other entities about possible identity theft in connection with covered accounts should be referred to the FACTA Compliance Coordinator. The FACTA Compliance Coordinator will see that appropriate mitigating responses as identified in section D.3 are followed.

4.) Suspicious activity - In the course of providing services and assistance to students and other customers, BYU employees will always seek to positively determine that the person whom they are assisting is in fact the individual they claim to be. Most suspicious activity, as identified in Section D.1 above will be encountered during these efforts. If requests for additional identifying information are unsuccessful, the BYU employee should deny further assistance and report the instance to the FACTA Compliance Coordinator. They should provide as much information as possible, such as the student name & ID in question, a description of the individual requesting access or assistance, date and time of the incident, the type of information or assistance requested, etc. The FACTA Compliance Coordinator will then see that appropriate responses, as identified in section D.3 are followed.

In attempting to identify students or customers who appear in person or contact BYU by phone, fax or email, the primary methods used for verification include:

a) In person – valid student ID or government issued ID for photo verification

b) Phone, fax or email – use of Challenge Questions such as:

i. Full name

ii. ID or Social Security Number

iii. Birth date

iv. Alternative addresses (home, permanent, mailing, prior, etc.)

v. Major program of study

vi. Classes currently enrolled

D.3 Responding to Red Flags – Prevention and Mitigation

Specific procedures for responding to detected Red Flags will vary with the degree of risk to the customer. Certain procedures for specific circumstances have already been identified. To determine an appropriate BYU response in all other circumstances, aggravating factors that may heighten the risk of identity theft will be considered. Such circumstances could include a) a data security incident that results in unauthorized access to a customer's account, b) notice that a customer has provided information related to a BYU covered account to an individual or website fraudulently claiming to represent BYU. Upon the detection of a Red Flag, BYU shall respond immediately and continuously until the integrity of an account and related charges are satisfactorily verified. Appropriate responses will include some or all of the following:

1.) Independently contact the customer using BYU contact information (this is the minimum response in virtually all circumstances)

2.) Monitoring a covered account for evidence of identity theft

3.) Change passwords, security codes, or other security devices that permit access to a covered account

4.) Re-open a covered account with a new account number

5.) Refuse to open a new covered account without independently contacting the customer using BYU contact information

6.) Close an existing covered account

7.) Not attempting to collect on a covered account through a debt collection agency without first verifying the validity of the charges and the obligation of the customer to pay

8.) Notify law enforcement of suspected identity theft

9.) Determine that no response is warranted under the particular circumstances.

D.4 Response protocol when identity theft is discovered

1.) Reportable vs. recordable identity theft events – BYU differentiates between reportable and recordable events. Any BYU employee, who becomes aware of a verified Red Flag, or an incidence of identity theft, shall report such to the FACTA Compliance Coordinator, who will then respond based on the definitions below:

a) **Reportable events** – These are identity theft events that have or could potentially affect a large number of customers; have or will likely be reported for criminal investigation; may require immediate response to avoid the compromise of additional personal information; or may require assistance from the ERMCC to ensure mitigation. These events will all be immediately investigated, logged and reported to the ERMCC.

b) **Recordable events** – These are identity theft events or identification of Red Flags that appear to be isolated; have not resulted in the actual, known compromise of personal information; give no indication of a systemic problem with BYU's data security or administrative procedures. These events will be investigated, as appropriate; and will be logged.

2.) The FACTA Compliance Coordinator will provide information regarding any immediately reportable event and the annual compliance report through normal reporting channels to the Administrative Vice President who will act as liaison to the ERMCC.

3.) The FACTA Compliance Coordinator shall notify the appropriate representative of BYU Police when an actual incidence of identity theft or a pattern of suspicious activity indicates a concerted effort to fraudulently obtain information from BYU or an attempt to change such information occurs.

E. Training & Communication

The FACTA Compliance Coordinator is responsible for designing and conducting training related to Red Flags. He/she is also responsible for managing communications regarding Red Flag and Identity Theft issues between individual departments and the ERMCC. Such training and communications shall include:

E.1 Training of BYU personnel

All BYU employees who work with personal information, as defined in Section B. above (Applicability), shall receive initial training related to Red Flags and the FACTA Compliance Program. This training may be supplemented as new information is received from regulatory agencies or as the FACTA Compliance Coordinator determines appropriate. The supplemental information may be disseminated in a formal training setting, as an on-line tutorial, or in the form of informational updates via email.

At some point, BYU may also elect to develop and require certification for those dealing with FACTA and Red Flag related issues. No such certification is currently required. However, a record of all employees trained will be maintained.

E.2 Communication

Any BYU employee who becomes aware of Red Flags, which have not been appropriately verified, and/or potential Identity Theft should communicate such immediately to the FACTA Compliance Coordinator. Such communication may be made in person, by phone, or by email. No formal written form is currently contemplated for this communication.

The FACTA Compliance Coordinator shall maintain a log of all reported Red Flags and/or Identity Theft. The log shall include indication of:

1.) Date

2.) Reported by

3.) Nature of Red Flag or identity theft

4.) Details of investigation

5.) Resolution

6.) Date reported to the ERMCC, if applicable

F. Monitoring and Reporting

F.1 Monitoring

At least annually, the FACTA Compliance Coordinator will meet with the department managers with FACTA compliance responsibility, as identified in Section B. above (Applicability), and review their FACTA compliance program, including their procedures for identifying, detecting, and responding to the Red Flags as defined in BYU's procedures. The results of these reviews will be included in the annual report to the ERMCC.

F.2 Oversight of Service Provider arrangements

Whenever BYU engages a service provider to perform an activity in connection with one or more covered accounts, BYU will take steps to ensure that 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. BYU will not generally dictate specific procedures, but will require that the

service provider provide a description of its procedures. The service provider shall also be required to report all known instances of Red Flags and identity theft, and their response and mitigation procedures to BYU. New and existing service provider agreements shall be reviewed and revised or amended to include language requiring the service provider to operate in accordance with the requirements of FACTA and the Red Flags rules. An annual review of service provider Red Flags procedures will be required of each service provider.

The following table identifies service providers currently performing services involving the use of personal information.

Service Provider	Type of service provided	
ECSI	Management of institutional student loans	
InfiNet	Management of on-line payments	
Cashnet	Cashiering systems	
General Revenue Corp	Collection Agency	
NCO	Collection Agency	
Williams & Fudge	Collection Agency	
EPN	Collection Agency	

F.3 Reporting

All Reportable events, as defined in D.4 1) a) above shall be reported immediately in writing to the ERMCC via the Administrative Vice President. The form of the reporting shall be appropriate to the situation but will include all information necessary to provide the ERMCC a full understanding of the situation and a recommended course of action.

Annually, the FACTA Compliance Coordinator shall provide the ERMCC with a report on compliance with the Program which shall include the following items:

1.) Summary of all reportable events, including response

2.) Summary of all recordable events, including response

3.) Summary of training conducted during the year

4.) Review of service provider compliance with Red Flag rules

5.) Recommended material changes in the Program or related procedures

G. Updating the Program

G.1 Circumstances warranting update of the Program

BYU will update the Program (including the Red Flags determined to be relevant) periodically, to reflect changes in risks to customers or to the safety and soundness of BYU from identity theft, based on factors such as:

1.) Prior experiences as identified in logs of Red Flags and identity theft cases.

2.) Changes of known methods of identity theft as well as changes in methods to detect, prevent, and mitigate identity theft. To identify such changes BYU will monitor trade association and regulatory agency updates and guidelines pertaining to Identity Theft.

3.) Changes in the types of accounts that BYU offers or maintains. As new services or opportunities are created that allow customers to obtain covered accounts, BYU will include these accounts in the review of identity theft risks.

4.) Changes in the way that BYU conducts business such as the expansion of the use of on-line services, use of third party service providers, etc.

G.2 Procedures for updating the Program

The annual report provided to the ERMCC will included proposed changes in text for the Program. Once approved, these changes will also be incorporated into all training materials.