VCU Identity Theft Prevention Policy

POLICY STATEMENT AND PURPOSE

In accordance with the Federal Trade Commission’s (FTC) Red Flag Rule 16 CFR Part 681, which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACT Act), it is the policy of Virginia Commonwealth University to establish an identity theft prevention program to detect, prevent, and mitigate identity theft in connection with new and existing covered accounts.

VCU is committed to identifying Red Flags associated with identity theft and protecting its students, faculty, staff, and others who entrust their personal information with the University. The University complies with the FTC Red Flag Rule by developing an identity theft prevention program that includes:

(1) Identifying and detecting “red flags”;
(2) Taking appropriate action when detection occurs to mitigate identity theft; and
(3) Updating the identity theft prevention program to reflect changes in risk.

WHO SHOULD READ THIS POLICY

All faculty and staff should read this policy.

RELATED DOCUMENTS

- VCU Identity Theft Prevention Program
- VCU Technology Services Computer Security Procedures and Standards
- VCU Police Identity Theft Precautions
- CFR Title 16: Part 681 Identity Theft Rules
- Section 114 of the FACT Act
- Section 615(e) of the Fair Credit Reporting Act (FCRA)

Initial Policy Approved by the Board of Visitors: 5/15/2009

Last Revised: 

Revision History:
CONTACTS

VCU Office of the Senior Vice President for Finance and Administration and the VCU Office of the Provost and Vice President for Academic Affairs officially interpret this policy and shall designate the University Information Security Officer to serve as the VCU Identity Theft Prevention Program Administrator. The Program Administrator will revise or eliminate any or all parts as necessary to meet the changing needs of Virginia Commonwealth University. Please direct policy questions to the Program Administrator.

TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Policy Statement and Purpose</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who Should Read This Policy</td>
<td>1</td>
</tr>
<tr>
<td>Related Documents</td>
<td>1</td>
</tr>
<tr>
<td>Contacts</td>
<td>1</td>
</tr>
<tr>
<td>Table of Contents</td>
<td>2</td>
</tr>
<tr>
<td>Definitions</td>
<td>2</td>
</tr>
<tr>
<td>VCU Identity Theft Prevention Program</td>
<td>3</td>
</tr>
</tbody>
</table>

DEFINITIONS

Covered Account

(1) An account that VCU offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and

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

Any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

Customer

A person that has a covered account with VCU. For the purpose of the VCU Identity Theft Prevention Program, all students, staff, faculty, and others having a covered account with VCU shall be referred to as “customer.”

Financial Institution

A state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that directly or indirectly holds a transaction account belonging to a customer.

Identity Theft

A 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 existence of identity theft.

VCU IDENTITY THEFT PREVENTION PROGRAM

I. Program Development and Adoption

VCU recognizes that some activities conducted by the University meet the definition of “creditor” and “financial institution” as defined by the Federal Trade Commission’s (FTC) Red Flag Rules, which implements Section 114 of the Fair and Accurate Credit Transactions Act (FACT Act). VCU is committed to conducting University business in compliance with federal law and after evaluating the nature and scope of the University’s activities subject to the “FTC Red Flag Rules,” the following program was developed.
This initial VCU Identity Theft Prevention Program (Program) was presented to the Student Affairs Committee of the VCU Board of Visitors for review and approval on May 14, 2009. As warranted the Program will be reviewed and updated to meet changes in risks associated with the detection, prevention, and mitigation of identity theft.

II. Program Purpose

The purpose of the Program is to detect, prevent, and mitigate incidents of identity theft in connection with VCU covered accounts as defined under the FTC Red Flag Rules. VCU is committed to identifying Red Flags associated with identity theft and protecting its students, faculty, staff, and others who entrust their personal information with the University.

III. The Program

In the development of the Program, existing policies, procedures, and internal controls that would limit reasonably foreseeable risks to our customers from identity theft have been included. We have also identified and evaluated the covered accounts that meet the criteria specified by the FTC for inclusion as a “covered account.”

IV. VCU Covered Accounts

Each University department is responsible for determining whether they have oversight for a covered account and must share that information with the Program Administrator for inclusion in the Program. Identified covered accounts at VCU are as follows:

a) **Student Installment Payment Plan Accounts**  
   *Responsible Office - Student Accounting*  
   A four payment installment plan offered to enrolled students during the Fall and Spring semesters with an administrative fee assessed. In order to participate, one fourth of the net total balance plus an installment plan fee must be paid.

b) **Student Deferred Payment Plan Accounts**  
   *Responsible Office - Student Accounting*  
   An extended payment plan offered to non-enrolled students through the semester following enrollment. The payment plan avoids referral to the VCU Collection Unit (Treasury Services) and additional collection costs. Thirty five percent of the outstanding balance must be paid and a payment schedule submitted before the proposed deferred payment plan is considered.
c) **Student Accounts with Refund Transactions**  
*Responsible Offices - Student Accounting/Treasury Services*

Refunds due to overpayment on account as a result of personal payments, financial aid, and/or third party sponsor awards. A refund is processed as a check to the student’s permanent address or parent’s address (PLUS loan Borrower); or as a direct deposit to the student’s bank account based on information submitted by the student on the direct deposit application form; or as a credit card payment return back to the credit card account used to make the payment. A refund may also be processed to a third party sponsor in the form of a check or credit card refund.

d) **Student Accounts in Collection with Payment Arrangements**  
*Responsible Office - Treasury Services*

Payment arrangements may be offered to non-enrolled students to collect a debt. A collection fee is assessed. Payment arrangements are generally set for the debt to be collected within six months.

e) **Loan Accounts**  
*Responsible Offices - Financial Aid/Treasury Services*

Federal Perkins Loans, Emergency Loans, University Loans, Nursing Student Loans, and Health Professions Loans are collected in accordance to the terms of the promissory notes. An outside billing service provider, Campus Partners is used to ensure due diligence for the above referenced loans with the exception of Emergency Loans.

f) **VCUCard Prepaid Declining Stored - Value Accounts**  
*Responsible Offices - Technology Services/VCUCard Office*

The VCUCard offers RamBucks, Meal Plans, Dining Dollars, Housestaff, Pay 4 Print, and Departmental Copy/Print prepaid declining stored-value accounts as part of the identification card. These accounts can be used at approved on campus and off-campus locations. Deposits can be made online with a credit card, depositing cash at an on campus CSVT, or by visiting a VCUCard office.

g) **Student Lockbox Payments**  
*Responsible Offices - Student Accounting/Treasury Services*

Student tuition and fee payments may be made via Wachovia Lockbox. Student Accounting invoices are mailed to student’s permanent mailing address with an envelope addressed to our processing center (lockbox) off-campus. Check, credit card; or
money order payments are accepted through the lockbox as are requests for enrollment in the installment payment plan.

h) **Credit Bureau Access**  
*Responsible Offices - Treasury Services/Human Resources*

Treasury Services accesses credit bureau information (view only) as a source for skip-tracing and verification of disputed credit bureau reporting on defaulted loans. HR utilization of credit bureaus is limited to credit history review of applicants and makes no updates of information of individuals based on this information.

V. **Service Provider Covered Accounts**

a) **VCUCard.** VCU has contracted with Wachovia to provide debit bank card services to customers having a VCUCard. As part of this Program, Wachovia’s information regarding their compliance with the FTC Red Flag Rules and their Identity Theft Prevention Program are included as Appendix A.

b) **Treasury Services.** VCU has contracted with Wachovia for lockbox services to students making tuition and fee payments; General Revenue Corporation, Williams and Fudge, and ConServe in the collection of past due loan, returned check, and tuition and fee accounts; and Campus Partners as a billing service provider in the collection of campus based student loans. As part of the Program, each institution’s information regarding their compliance with the FTC Red Flag Rules and their Identity Theft Prevention programs are attached. See Appendix A, B, C, D, and E respectively.

VI. **Identification of Relevant Red Flags**

a) **Risk Factors.** To identify potential red flags associated with covered accounts at VCU, the following will be considered:

- The types of covered accounts offered by VCU;
- The methods provided or employed to open a covered account;
- How customers can access covered accounts; and
- Any previous experiences with identity theft.

The following information sources are used in creation of covered accounts at VCU. Staff should evaluate this information and the methods used in collection of this information for “red flags.”
• Common application (admissions/loan) with personally identifying information
• Transcripts
• Official standardized test scores
• Letters of recommendation
• Application for Virginia Domicile
• Medical/Immunization Record
• Loan Application/Promissory Note
• Direct Deposit Form
• New hire process

b) Sources of Red Flags. VCU staff should incorporate relevant Red Flags from the following sources:

• Incidents of identity theft experienced by VCU;
• Methods of identity theft identified by VCU that signal a change in risks; and
• Applicable guidance.

c) Categories of Red Flags. The University has identified the following Red Flags in each of the categories listed below:

i) Notifications and Warnings from Credit Reporting Agencies

- Alerts, notifications, or other warnings; and
- Reports of fraud from consumer reporting agencies or service providers.

ii) Suspicious Documents

- Receipt of suspicious documents (such as an identification card) that appear fraudulent, or is presented by a person who does not fit the photograph/description on the identification card;
- Presentation of other documentation that is inconsistent with existing information; and
- Application or other documentation appears to be forged or altered.

iii) Suspicious Personal Identifying Information
- Identifying information presented that was previously presented by another person;
- Identifying information that is inconsistent with other sources of information for the same person;
- Identifying information that was previously found to be fraudulent; and
- Failure to provide complete identifying information as requested.

iv) Suspicious Covered Account Activity or Unusual Use of Account

- The unusual use of, or other suspicious activity related to a VCU covered account;
- Unusual requests to make changes to account information;
- Attempts to redirect refund monies from the destination identified in the system of record;
- Attempts to involve the university in the verification of the identity of the account holder to an external entity; and
- Unauthorized access to or use of a customer’s information or covered account.

v) Alerts From Others

- Notice received from customers, victims of identity theft, law enforcement authorities or others regarding possible identity theft associated with a VCU covered account.

d) Detecting Red Flags. VCU staff should implement policies and procedures to address the detection of Red Flags associated with opening a covered account or accessing an existing covered account. The following procedures will be used in detecting Red Flags:

- Obtain and verify the identity of a customer opening a covered account;
- Authenticate customers when making changes to an existing covered account;
- Monitor transactions for possible Red Flags; and
- Verify the validity of a change of address request on an existing account and provide the customer with a means to promptly report an incorrect address.

VII. Procedures to Mitigate Identity Theft
The Program includes the following University general and student accounting procedures to mitigate identity theft. Additional procedures should be developed as necessary to address specific covered accounts.

**General Procedures:**

**a)** Require certain identifying information such as name, birth date, academic records, home address, and other identification before creating a new account. Check for inconsistent or incomplete information and do not activate the account unless you receive complete information.

**b)** Verify the customer’s identity at the time an identification card is issued (review driver’s license, passport, or other government issued photo id).

**c)** Encourage customers to make changes of address through the appropriate password protected system or when applicable the Self Service Banner System (requires knowledge of eID and password). If requested in person, require picture identification;

**d)** Ensure that paper documents associated with or containing covered account information and customer personally identifiable information are maintained in a secure environment and are shredded when retention requirements expire.

**e)** Ensure that electronic files containing covered account information and customer personally identifiable information are secured in accordance with University information security requirements, and that access to such files is limited to those who need access to perform their job duties and that such files and records within them are securely destroyed when retention requirements expire.

**f)** Ensure that University websites used to access covered accounts meet University information security requirements.

**g)** Collect social security numbers only if required or authorized by federal or state law or authorized by the University Information Security Officer.

**h)** Require a student to identify himself/herself with picture identification and/or student number before providing him/her information about his/her student account.
Refund Processing Procedures:

i) Check refunds must be sent to the active address indicated in the Banner System, and the PLUS parent address collected on the application by the Financial Aid Office. Students/parents cannot request a check to be sent to a different address, the address in the system must be used.

j) Direct Deposit refunds must be sent to the account submitted by the customer on the Direct Deposit Form and voided check. An email notification will be sent to the customer’s VCU email address notifying him/her of the refund when the direct deposit is processed.

k) Credit card refunds are required to be processed back to the same account used for payment.

Installment and Deferred Payment Plans Procedures:

l) For the installment payment plan, a minimum payment of 25% of the balance plus an installment fee is required for participation. For the deferred payment plan, a minimum payment of 35% of the outstanding balance must be paid before the request is considered. The student number must be provided when making the request.

VIII. Response to Red Flag Detection

In determining the possible responses to Red Flags associated with VCU covered accounts, factors that may increase the risk of identity theft were considered. Based on these considerations, if red flags are detected, one or more of the following steps should be taken:

a) Change passwords or disable access to covered accounts after notifying student;

b) Investigate transactions to covered accounts which include contacting the actual customer to notify the customer and verify if activity is fraudulent;

c) Close the covered account;

d) Reopen a covered account with a new account number after inactivating the existing account number;

e) Do not open a new covered account for the customer;
f) Notify the Program Administrator;

g) Notify law enforcement; and

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

IX. Program Administration

a) Oversight of the Program. The FTC Red Flag Rules require that provisions be made for the oversight, development, implementation, and administration of the Program. This requirement may be met by an entity’s board, appropriate committee of the board, or a designated employee at the level of senior management. The Office of the Senior Vice President for Finance and Administration and the Office of the Provost and VP for Academic Affairs designate the University Information Security Officer to implement and oversee the VCU Identity Theft Prevention Program.

b) Reports. At least annually, the Program Administrator will require and review reports submitted by staff on the compliance of VCU with the Program. These reports should address and evaluate the following:

- Material matters related to the Program;
- Effectiveness of policies and procedures in addressing the risk of identity theft in connection with the opening of covered accounts;
- Service provider arrangements;
- Significant incidents of identity theft and management response; and
- Recommendations for changes to the Program.

c) Updating the Program. The Program Administrator will update the Program periodically to reflect changes in risks to customers or to the safety and soundness of VCU based on the following factors:

- VCU experiences with identity theft;
- Changes in methods of identity theft;
- Changes in methods available to detect, prevent, and mitigate identity theft;
- Changes in the types of covered accounts maintained by VCU; and
• Changes in business arrangements such as alliances, joint ventures, or service provider agreements entered into by VCU.

d) **Staff Training and Reporting.** The Program Administrator will ensure that employees responsible for activities associated with the creation of covered accounts receive training on the detection of Red Flags and the appropriate response when a Red Flag is detected.

e) **Oversight of Service Provider Arrangements.** In instances where the University contracts for services provided in association with a covered account, VCU will require that the service provider has reasonable policies and procedures in place to detect, prevent, and mitigate the risk of identity theft. Additionally, documentation supporting the existence of policies and procedures or an identity theft prevention program shall be acquired and implemented into the Program.
Appendix A

November 6, 2008

Effective November 1, 2008, all banks were required to have appropriate policies and procedures in place to comply with the new Identity Theft Prevention Program rules, which are also known as the “Red Flag Rules”. Wachovia has reviewed its policies and procedures concerning fraud and identity theft to verify that the policies and procedures address the requirements of the Red Flags Rules, and has documented its Identity Theft Prevention Program (the “Program”) in accordance with the Red Flags Rules. Wachovia Corporation’s Board of Directors has approved the Program.

The key components of the Program include policies and procedures designed to:

- 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;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Ensure periodic updates to the Program to reflect changes in risks from identity theft.

The Program utilizes policies and procedures maintained by lines of businesses as well as enterprise-wide corporate policies and procedures in areas such as:

- Anti-Money Laundering and Anti-Terrorist Financing
- Loss Management
- Information Security
- Supplier Risk Management

Wachovia has always been committed to protecting customer information, and Wachovia already had a strong identity theft prevention program in place prior to publication of the Red Flags rules. For example, Wachovia employees are trained on the relevant policies and procedures for protecting customer information and preventing fraud and identity theft. In addition, employees are held accountable by Wachovia’s Code of Conduct and Ethics to properly protect customer information.

The products and services delivered by Wachovia to its customers are provided in accordance with policies and procedures designed to detect, prevent and mitigate identity theft and fraud in compliance with the Red Flags Rules.
Did you know?

Last year, The Federal Trade Commission (FTC) and Federal banking agencies issued a regulation known as the Red Flag Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act (FCRA), effective November 1, 2008. Please note: Sallie Mae has met the November 1 deadline; however on October 22, 2008, the FTC gave creditors and financial institutions until May 1, 2009 to comply. Other federal agencies are abiding by the November 1, 2008 date.

Why Is this Important?

The rule requires creditors and financial institutions offering or servicing covered accounts to develop and implement a written Identity Theft Prevention Program for new and existing accounts. The program must:

- Identify the Red Flags relevant to the organization and its operations, which must be incorporated into the program;
- Have the ability to detect the Red Flags the program identifies;
- Have procedures in place to respond appropriately to any detected Red Flags to prevent and mitigate identity theft; and
- Reflect changes in risks to customers or to the safety and soundness of the institution from identity theft via periodic updates.

Sallie Mae's written FACTA Identity Theft Prevention and Red Flags Program, which applies to all subsidiaries (including General Revenue Corporation) was approved by the Sallie Mae Board of Directors, is comprehensive and meets the requirements of the FACTA. To learn more about Sallie Mae's security and fraud prevention measures and how it safeguards you and your borrowers, please refer to the attached fact sheet.

If you have additional questions or concerns about FACTA or the Red Flag Rule, please contact any GRC Client Service Representative, Account Manager or Sales Executive.
The FACT Act
Identity Theft Prevention Program

A Letter to Our Valued Customers and Clients:

As the nation's leading provider of student loans and administrator of college savings plans, Sallie Mae® understands the importance of protecting the identity of those who entrust their personal information to us, as well as ensuring appropriate measures are taken to prevent identity theft.

Last year, the Federal Trade Commission (FTC) and Federal banking agencies issued a regulation known as the Red Flag Rule under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act (FCRA). The Red Flag Rule was intended to reduce the risk of identity theft and takes effect November 1, 2008. Compliance is mandatory for creditors or financial institutions that provide “covered accounts,” defined by the rule as personal, family or household accounts, or any other account in which there is a reasonably foreseeable risk of identity theft. The rule identifies a number of patterns, practices and specific forms of activity that are “Red Flags,” signaling the possibility that identity theft may be taking place.

The rule requires creditors and financial institutions offering or servicing covered accounts to develop and implement a written Identity Theft Prevention Program for new and existing accounts. The program must:

- Identify the Red Flags relevant to the organization and its operations, which must be incorporated into the program;
- Have the ability to detect the relevant Red Flags the program identifies;
- Have procedures in place to respond appropriately to any detected Red Flags to prevent and mitigate identity theft; and
- Reflect changes in risks to customers or to the safety and soundness of the institution from identity theft via periodic updates.

The FACTA also requires credit card and debit card issuers to develop policies and procedures to assess the validity of a change of address notification followed closely by a request for an additional or replacement card. In addition, the Red Flag Rule requires financial institutions or creditors that use consumer reports to develop reasonable policies and procedures regarding notices of address discrepancies they may receive from a consumer reporting agency when a credit report is obtained.
The Sallie Mae FACTA Identity Theft Prevention and Red Flags Program

Ensuring that appropriate security and fraud prevention measures are in place to protect our customers and to prevent identity theft has always been an important aspect of Sallie Mae’s business operations. We are proud of the safeguarding programs we have developed and the trust that our customers and clients have placed in us.

We are pleased to share that Sallie Mae has been, and will continue to be, in compliance with both the FACTA and the Red Flags Rule. In response to the regulations, Sallie Mae has taken and completed the following initiatives:

- We established a Corporate FACTA Compliance Committee and appointed Roy Mellinger, Vice President and Chief Security Officer for the corporation to oversee the program.
- We developed and published a Corporate FACTA Program Manual that provides enterprise guidance to all our lines of business, including details on detecting and responding to Red Flags.
- Every line of business participated in identifying Red Flags relevant to its specific operations, confirming it has manual and automated processes to detect and respond to relevant Red Flags, and providing documentation to verify its well-written procedures defining the processes and response strategies.
- We have consolidated all relevant Red Flags identified by our lines of business into an organizational matrix to ensure appropriate governance and oversight at the highest levels of the corporation. This information, and the state of our Red Flags compliance program, is routinely communicated to senior management and shared with the Sallie Mae Corporate Compliance Committee, chaired by James Truitt, Senior Vice President of Corporate Compliance.
- We developed and provided FACTA and Red Flags awareness training materials to all our lines of business, and in turn asked that they provide Red Flags training to all employees and staff who require that information, and we asked that this training be documented and centrally reported.

Sallie Mae’s written FACTA Identity Theft Prevention and Red Flags Program, which was approved by the Sallie Mae Bank Board of Directors, is comprehensive and meets the requirements of the FACTA. Contact your Sallie Mae liaison or point of business contact for more information about our FACTA Identity Theft Prevention and Red Flags Program.
Appendix C

Williams & Fudge, Inc.
Identity Theft Prevention Safeguards
Red Flag Rules

Introduction:
The Federal Trade Commission (FTC) along with the federal bank regulatory agencies, and the National Credit Union Administration (NCUA) issued new regulations in 2008 to enforce the FACT Act (Fair and Accurate Credit Transaction) of 2003. Commonly referred to as “Red Flag Rules”, all financial institutions and creditors are required to develop a written program that identifies potential opportunities for identity theft, as well as procedures and policies in place to prevent, detect, and respond to patterns, practices, or activities that could indicate identity theft.

Although Williams & Fudge, Inc. does not extend credit, it is prudent to establish policies and procedures to prevent identity theft under the definition of “creditor.” Simply stated, Williams & Fudge, Inc. is committed to intent of the Red Flag Rules and understands their importance to its clients.

Purpose:
Williams & Fudge, Inc. has written procedures in place to identify and respond to identity theft in connection with the collection of defaulted accounts that have been referred to our office for collections. Our office is operating in the capacity of third party collections.

Encompassing Parties:
The policy and safeguards pertain to all Williams & Fudge, Inc. employees who have direct access to personal information of any account record that is submitted by our clients.

Definitions:
Identity Theft: Any individual or organization that uses the identity of another person for the purpose of committing fraud.

Red Flags: Any pattern, practice, or activity that could indicate the possible risk of identity theft.

Identifying Information: Any personal data that may be used to identify an individual. This information may include name, social security information, student identification, financial data, address, and date of birth.
Policies & Procedures:

Red Flag Alerts

a. Upon receipt of any non electronic account placement media, the Client Support Department (responsible department) will review and scrutinize all documents for identification of any possible red flags;

b. Upon receipt of any non electronic account support documentation that may include parental or relative information, debt documents including account ledgers, promissory notes, the Client Support Department and/or the Collection Representative who received the information will review and scrutinize all documents for identification of any possible red flags;

c. Upon receipt of any electronic account placement media, the Client Support Department and/or the Conversion & Program Development Manager will review and scrutinize all data fields for identification of any possible red flags, and;

d. Upon receipt of any electronic support documentation that may include parental or relative information, debt documents including account ledgers, promissory notes, the Client Support Department and/or the Conversion & Program Development Manager will review and scrutinize all data fields for identification of any possible red flags.

Red Flags Include:

a. Documents and or files that provide identifying information that may appear to be altered, substituted, or forged;

b. Any descriptive information that may be defined as identify as described above that is not consistent with previous information provided by the clients or received from the consumer (debtor);

c. Social Security number as submitted by the client or consumer (debtor) that is associated with known fraudulent activity and/or is inconsistent;

d. Social Security number as submitted by the client or consumer (debtor) that is the same as another account or file record;

e. Account Ledgers, promissory notes and any personal references that is inconsistent with identifying information;

f. Any financial information including banking information, or any other payment medium that will be used for repayment of the debt that is inconsistent with existing identify information;

g. Any personal identifying information received from third party skip-tracing vendors that are inconsistent with existing identifying information. Other than inconsistencies in the industry such as address changes;

h. Any voice mail, email, text, or fax that includes and/or encloses any personal identifying information or financial information that may be inconsistent with existing identifying information; and

i. Any voice mail, email, text, or fax that includes and/or encloses any personal identifying information or financial information that may be known to be identified with fraudulent activity.
Prevention and Mitigation Procedures Regarding The Placement Of New Accounts (Non-Electronic):

a. Upon receipt of placement media (non-electronic) and following scrutinizing of all identifying information, any identification information as described previously that may appear to be fraudulent and/or inaccurate will be brought to the attention of the client for verification;

b. If the appropriate personnel is unable to obtain satisfactory verification of identifying information from the client, the media (account record) will be recorded and submitted to:
   i. The Department Manager/Supervisor; or
   ii. The Compliance Officer;

c. No flagged record will be updated and/or added to the system without complete investigation and assurance that the identifying information is accurate; and

d. If appropriate proper law enforcement will be notified of any fraudulent attempts.

Prevention and Mitigation Procedures For Placement Of New Accounts (Electronic):

a. Upon receipt of data-file (electronic), all conversion will be loaded and reviewed in a test mode prior to a live load onto the computer system;

b. Following scrutinizing of all identifying information within the data fields, any identification information as described previously that may appear to be fraudulent and/or inaccurate will be brought to the attention of the client for verification;

c. If the appropriate personnel is unable to obtain satisfactory verification of identifying information from the client, the media (account record) will be recorded and submitted to:
   i. The Department Manager/Supervisor; or
   ii. The Compliance Officer;

d. No flagged record will be loaded, updated and/or added to the system without complete investigation and assurance that the identifying information is accurate; and

e. If appropriate proper law enforcement will be notified of any fraudulent attempts.

Prevention and Mitigation Procedures For Placement And/Or Receipt Of Support Documentation For Existing Accounts (Non-Electronic):

a. Upon receipt of placement and or support documentation media (non-electronic) that includes such identifying information as parent or relative information, debt documents including account ledgers, promissory notes, and/or any other personal identifying information will be loaded and reviewed in a test mode and scrutinized for any information that may appear to be fraudulent and/or inaccurate;
Appendix D

CONSERVE
PROFESSIONAL PRACTICES MANAGEMENT SYSTEM

PROCEDURE FOR RESPONDING TO RED FLAG NOTICES & DOCUMENTING THE IDENTITY OF A CONSUMER
CP NUMBER 904

Approved By: Pamela Keleher & Pamela Baird
Written By: Pamela Keleher & Pamela Baird
Date: October 1, 2008

PROCEDURE FOR RESPONDING TO RED FLAG NOTICES AND DOCUMENTING THE IDENTITY OF A CONSUMER (904)

1.0 PURPOSE

The purpose of this procedure is to comply with New York State Legislation (Senate Bill 7297) regarding handling consumer claims of Identity Theft and the Federal Trade Commission (FTC) Red Flags Rule (16 C.F.R. §681.1 and §681.2).

ConServe is not an entity required to create a program under the Red Flags Rule. For example, ConServe is not an entity that regularly extends, renews, or continues credit. ConServe does not regularly arrange for the extension, renewal, or continuation of credit and it does not participate in the decision to renew or continue credit.

However, by creating procedures to respond to these laws, ConServe will assist its Clients with responding to Identity Theft.

2.0 SCOPE

This procedure covers all accounts at ConServe.

3.0 DEPARTMENTS RESPONSIBLE FOR IMPLEMENTATION

Production & Production Support Departments & Compliance

4.0 GENERAL

On August 5, 2008, New York Governor David Paterson signed into law Senate Bill 7297, which established procedures related to Identity Theft. This law is effective September 1, 2008.

In 2007, the Federal Trade Commission (FTC) and Federal banking agencies issued regulations known as the Red Flags Rule intended to respond to and reduce the risk of Identity Theft. Mandatory compliance with the Red Flags Rule for “creditors” or “financial institutions” that provided “covered accounts” begins on November 1, 2008.

As to the Red Flags Rule, this procedure will:

- Identify what Red Flags are;
- How ConServe will respond to Red Flags; and
- How often ConServe will update this program

5.0 PROCEDURE

5.1 Identification of Red Flags

Red Flags include the following:

- A notice from a consumer as a victim of Identity Theft, law enforcement authorities, or other persons regarding possible identity theft in connection with an account.
- Alerts, notifications, or other warnings received from consumer reporting agencies or service
5.2 Responding to Identity Theft Claims Directly from Consumers or Credit Reporting Agencies

5.2.1 Verbal Notification:
When a debt counselor receives verbal notification from a consumer that he or she is a victim of Identity Theft, the debt counselor will ask the consumer to provide a copy of a police report filed by the consumer alleging the consumer is a victim of Identity Theft for the specific account(s) being collected.

In addition, the debt counselor should place the account into 3IDP (Possible Identity Theft) disposition to await the documentation.

NOTE: If the account has been reported, disposition 3IDP (Possible Identity Theft) will update the tradeline on the consumer's credit report as 'disputed' (if the account has been reported).

In addition, when the account is moved to disposition 3IDP, a tactic will systematically generate Letter 3052 to request a police report from the consumer & for the consumer to complete an Identity Theft Form Affidavit (CF Number 904-1).

5.2.2 Written Notification:
Upon receipt of a consumer's written notification of Identity Theft, Production Support will update the notepad.

If the written Identify Theft claim does not include a police report, then the account will remain in disposition 3IDP (Possible Identity Theft) or put into this disposition if we have not made prior verbal contact with the consumer. In addition, Production Support will request FACS letter number (Letter 3502) to request a police report from the consumer and that the consumer complete the Identity Theft form affidavit (CF Number 904-1).

Upon receipt of a valid police report and completed Identity Theft Form Affidavit (CF Number 904-1), our office must cease collection activity.

Production Support will (1) update the disposition to 3IDT (Identify Theft) to prevent any further calls or letters and update the notepad with this information and (2) forward this information to our Client using FACS letter number (Letter 3500) to review & advise.

NOTE: If the account has been reported, disposition 3IDT (Identity Theft) will update the tradeline on the consumer's credit report as 'disputed' (if the account has been reported).

5.2.3 Notification from Consumer Reporting Agency (CRA):
Upon receipt of a consumer Identify Theft claim via E-Oscar, or a dispute that reveals the disputing consumer's information is different than ConServe's information, Production Support, will update the credit flag as a dispute and update the notepad with this information.

In addition, Production Support will update the disposition 3IDP (Possible Identity Theft) and request FACS
letter number (Letter 3052) to request a police report and an Identity Theft Form Affidavit (CF Number 904-1) from the consumer.

Upon receipt of a valid police report and completed Identity Theft Form Affidavit (CF Number 904-1), our office must cease collection activity. Therefore, Production Support will update the status code to 3IDT (Identity Theft) to prevent any further calls or letters and update the notepad with this information. In addition, this information is forwarded to our Client using FACS Letter 3500 to review & advise.

5.2.4 Client Response:
We may only resume collection activity if our Client advises us in writing that the information provided by the consumer and other sources does not establish Identity Theft occurred.

Upon receipt of this written documentation from our Client, Production Support will send out FACS Letter Number (Letter 3053) advising the consumer of the Client’s decision to resume collection activities.

After this letter is mailed, a tactic will run to change the disposition from 3IDT (Identity Theft) to disposition 3001 (New Information) after five (5) days. This will allow time for the consumer to receive notification of the Client’s decision prior to resuming collection activity.

If our Client indicates that it is a valid claim of Identity Theft, then Production Support will cancel the account (9000) using cancel code: FRD (Fraud).

5.3 Verifying the Identity of the Person With Which You Speak
Our debt counselor’s are required to properly identify the consumer in accordance with ConServe’s policy before discussing the existence of a debt by:
- Verifying consumer by Social Security Number, or
- Verifying consumer by Date of Birth, or
- Verifying consumer by school

5.5 Updating this Procedure
Review of this procedure will occur annually. Updates will occur as needed using the PPMS Document Change Process.

5.6 Administration of this Procedure
Oversight of this procedure will be provided by the Vice President of Privacy & Compliance Officer. The responsibilities for oversight will include assigning specific responsibility for the Training of staff to administer the implementation of this procedure will occur immediately, annually and as needed for updates.

6.0 RECORDS
All written correspondence received regarding the Identity Theft claim will be scanned to the account in W47 in FACS.

7.0 FORMS
CF Number 904-1 Identity Theft Form Affidavit
8.0 DEFINITIONS

*Red Flag Notice* means:

- A notice from a consumer as a victim of Identity Theft, law enforcement authorities, or other persons regarding possible identity theft in connection with an account.
- Alerts, notifications, or other warnings received from consumer reporting agencies or service providers including fraud or activity alerts with a consumer report, a notice of credit freeze from a consumer reporting agency, a notice of address discrepancy from a consumer reporting agency.
- The presentation of suspicious documents, such as those that appear to have been altered or forged.
- Information provided by the consumer in a dispute does not match information ConServe has on file from a client.

*Personally Identifiable Information* means information that is stored in electronic or printed format which is the Consumer’s:

a. First, middle, or last name  
b. Date of birth  
c. Address  
d. Telephone or wireless numbers  
e. Social Security Number  
f. Government issued identification number  
g. Maiden name  
h. Account number  
i. Credit card information including card number, expiration date, cardholder name and cardholder address  
j. Medical information including doctor’s names, insurance claims, prescriptions, treatment and diagnosis and any related personal medical information

9.0 REFERENCE DOCUMENTS

ACA PPMS:2000 Element 9
Appendix E

STUDENT LOANS

Identity Theft Prevention Program
Red Flag Guidelines - Campus Partners

Summary:

The Financial Institution Regulators, including the Federal Trade Commission (FTC), have issued a final rule (the “Red Flag Rule”) under sections 114 and 315 of the Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act (FCRA). The Red Flag Rule requires “financial institutions” and “creditors” that hold “covered accounts” to develop and implement an identity theft prevention program for new and existing accounts. The Red Flag Rule also addresses service provider arrangements. Guidelines issued under the Red Flag Rule make it clear that a service provider such as Campus Partners that provides services to multiple financial institutions and creditors may have its own program to prevent identity theft so long as it meets the requirements of the rule.

Campus Partners takes the possibility of identity theft seriously and, in full compliance with the Red Flag Rule, has developed and implemented an Identity Theft Prevention Program.

Risk Assessment:

Campus Partners’ executive management staff, working together with our legal counsel, has conducted a risk assessment to determine where the potential lies for risk in the different areas of our operations.

Risk Factors:

Financial Risks with Respect to Identity Theft - Private Loans: We have identified the following risks for the Private Loan Programs that are originated by Campus Partners:

1. The applicant attempts to secure loan funds using another individual’s identity.
2. The applicant attempts to secure loan funds with fraudulent income verification and/or fraudulent school certification.
3. The applicant attempts to secure loan funds and provides information about a co-signer without that person’s knowledge or consent.
4. A co-signer applies for loan funds using the identity of a primary applicant without that person’s knowledge or consent.

Many of these risks are addressed by Campus Partners’ previously approved Customer Identification Program, which is incorporated into our Identity Theft prevention Program.
Financial Risks with Respect to Identity Theft – Campus-Based Federal Loans and Institutional Loans – Campus Partners does not arrange for the extension, renewal, or continuation of credit with respect to Campus-Based federal loans (including Federal Perkins Program Loans) and institutional loans it services. The Red Flag Rule does not generally apply to the servicing activities performed on these loans. All loans are funded prior to the boarding of loans on our servicing system.

Operational and Reputation Risks:

1. Access to Account Information by Third Parties – For all loan programs serviced by Campus Partners, Campus Partners has incorporated a program to authenticate borrowers into its procedures to prevent unauthorized access to account information. This applies to access through our Interactive Voice Response system (IVR), our borrower website (mycampusloan.com), by calling and speaking with a representative, or through written correspondence.

2. Access to Account Information by Campus Partners’ Staff – Our Human Resources department conducts a criminal background check on all new personnel. New employees are required to attend Security Awareness training conducted by our Chief Security Officer. All employees are counseled about the confidential nature of the information, our clear desk policy, Internet security and usage, and other company confidentiality policies and procedures. Employees are required to sign a non-disclosure agreement as a condition of employment.

Red Flags

Based on these identity theft risks, Campus Partners has developed Red Flags which serve as indicators of possible identity theft. Our Identity Theft Prevention Program describes how we detect the presence of these Red Flags and how we respond to detected Red Flags in order to mitigate identity theft.