Identity Theft Prevention - Interim

Policy Type: Board of Visitors
Responsible Office: Vice President of Administration and the Provost and Vice President for Academic Affairs
Initial Policy Approved: 05/15/2009
Current Revision Approved: 04/23/2018

Policy Statement and Purpose

VCU is committed to protecting the information of its students, faculty, staff, and others who entrust their personal information to the university. 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 and maintain an Identity Theft Prevention Program to detect, prevent, and mitigate identity theft in connection with new and existing covered accounts.

This policy and the documents listed in the Related Documents section constitute the primary components of VCU's Identity Theft Prevention Program.

Noncompliance with this policy may result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation is prohibited.

Table of Contents

Who Should Know This Policy

All employees (includes faculty, university and academic professionals, and staff) and students are responsible for knowing this policy and familiarizing themselves with its contents and provisions.

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 will 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.

Identifying Information

Identifying information means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person, including any —

(1) Name, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number;

(2) Unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation;

(3) Unique electronic identification number, address, or routing code; or

(4) Telecommunication identifying information or access device (as defined in 18 U.S.C. 1029(e))."

See 16 C.F.R. ' 603.2(b).

Identity Theft
A fraud committed or attempted using the identifying information of another person without authority.

Identity Theft Prevention Program Administrator (Program Administrator)
The Identity Theft Program Administrator is the individual responsible for the development, documentation, execution, and monitoring of VCU's Identity Theft Prevention Program.

Identity Theft Prevention Standard
The Identity Theft Prevention Standard outlines the operational requirements of the Identity Theft Prevention Program as established by the Identity Theft Prevention Policy. This standard is developed, revised, and maintained by the Technology Services' Information Security Office in consultation with the university's Technical Advisory Committee and all identified stakeholders.

Red Flag
A pattern, practice, or specific activity that indicates the possible existence of identity theft.

Contacts

The Division of Administration and the Office of the Provost and Vice President for Academic Affairs officially interpret this policy and shall designate the Chief Information Security Officer to serve as the VCU Identity Theft Prevention Program Administrator. Please direct policy questions to the Identity Theft Prevention Program Administrator (itppadmin@vcu.edu).

Policy Specifics and Procedures

A. Program 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 to this end has established the creation and maintenance of an Identity Theft Prevention Program with an assigned Program Administrator. The Identity Theft Prevention Program includes the Identity Theft Prevention policy, Identity Theft Prevention Standard, all other associated standards and related documents. All departments having covered accounts must adopt and follow the Identity Theft Prevention Policy and its associated Identity Theft Prevention Standard and Identity Theft Prevention Program.

B. Program Content
VCU is committed to identifying "red flags" associated with identity theft and protecting its students, employees, and others who entrust their personal information with the university. The university complies with the FTC Red Flag Rule by developing and maintaining an Identity Theft Prevention Program that includes:

- VCU Covered Accounts

  Each university department is responsible for determining whether they have use, manage, or oversee covered accounts and must identify covered accounts to the Program Administrator. Departments are also responsible for notifying the Program Administrator when they no longer have oversight for a covered account. Each department having a covered account must assign a departmental contact and provide the Program Administrator with the contact's name, email address and phone number.

  Please see the Identity Theft Prevention Standard for a list of acknowledged covered accounts at VCU

- Service Provider Covered Accounts

  Each university department is responsible for determining whether they intend to contract with a service provider who will use, manage, or oversee covered accounts and must identify service provider covered accounts to the Program Administrator. Departments are also responsible for notifying the Program Administrator when they no longer have a contract that establishes a service provider covered account. Each department having responsibility for a service provider covered account must assign a departmental contact and provide the Program Administrator with the contact's name, email address and phone number.

  Please see the Identity Theft Prevention Standard for a list of acknowledged service provider covered accounts at VCU.

- Identification of Relevant Red Flags

  Departments using, managing or overseeing covered accounts and service provider accounts are expected to develop and maintain processes in identifying relevant red flags. These processes must follow guidance provided through the Identity Theft Prevention Standard and takes the following items into consideration:

  - 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 the creation of covered accounts at VCU. Departments should evaluate this information and the methods used in collection of this information for red flags.

Common applications (admissions/loan/hr) 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 Forms (including Direct Deposit, Federal and State Tax Forms, Tax Deferred Annuity, Deferred Compensation, Designation of Beneficiary, Health Benefits and Visa information).

- Sources of Red Flags
  Responsible offices must 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.

- Categories of Red Flags
  The university has identified and documented red flags by category in its Identity Theft Prevention Standard. Responsible offices are expected to consult with the documented categories in the Identity Theft Prevention Standard when developing and reviewing processes for identification of red flags.

- Detecting Red Flags
  The university has listed general procedures to detect red flags in its Identity Theft Prevention Standard. Responsible offices are expected to consult with the documented categories in the Identity Theft Prevention Standard when developing and reviewing processes for identification of red flags.

- Procedures to Mitigate Identity Theft
  Responsible Offices must comply with the Identity Theft Prevention Program, including the following university general and student accounting procedures to mitigate identity theft. Responsible offices in collaboration with the Program Administrator may develop additional procedures and revise existing procedures to mitigate identity theft. All identity theft mitigation procedures must be documented in the Identity Theft Prevention Standard.

- Respond 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 must be considered. Based on these considerations, if red flags are detected, Responsible Offices must notify the Program Administrator (itppadmin@vcu.edu) and take the following steps:

1. Temporarily suspend access to the covered account and require a password change from the customer.
2. Investigate transactions to covered accounts that include contacting the actual customer to notify the customer and verify if activity is fraudulent
3. Close the covered account
4. Reopen a covered account with a new account number after inactivating the existing account number
5. Do not open a new covered account for the customer
6. Notify law enforcement
7. Determine that no response is warranted under the particular circumstances

C. Program Administration, Development and Maintenance

The Vice President for Administration and the Provost and VP for Academic Affairs designate the university's Chief Information Security Officer to oversee the VCU Identity Theft Prevention Program. The Chief Information Security Officer may delegate the administration of the Identity Theft Prevention Program to a designated Program Administrator. The designated Program Administrator in collaboration with departments that use, manage, or oversee covered accounts and service provider accounts will be responsible for the implementation of the Identity Theft Prevention Program.

In the development and maintenance of the Identity Theft Prevention Program, policies, standards, procedures, and internal controls that limit reasonably foreseeable risks to VCU's customers from identity theft must be included. The Program Administrator must identify and evaluate the covered accounts that meet the criteria specified by the FTC for inclusion as a "covered account." The Program Administrator must document the Identity Theft Prevention Program, identify stakeholder participants, establish communication with and training for stakeholder participants, and monitor program compliance in accordance with the VCU Identity Theft Prevention Program Standard. The Program Administrator is responsible for revising or eliminating any or all parts of the VCU Identity Theft Prevention Program as necessary to meet the changing needs of Virginia Commonwealth University and applicable laws and regulations.

Forms

VCU Information Security Exception Form

Related Documents

1. VCU Identity Theft Prevention Program Standard [link to be added when available]

2. VCU Technology Services Policies, Standards, Baselines and Guidelines

https://ts.vcu.edu/askit/policies-and-publications/information-technology-policies-standards-baselines--guidelines/

3. VCU Police Identity Theft Prevention Recommendations
https://police.vcu.edu/stay-safe/identity-theft-prevention/

4. CFR Title 16: Part 681 Identity Theft Rules
https://www.ecfr.gov/cgi-bin/text-idx?SID=054b71cf91182598d8b6ef525fd04fef&mc=true&node=pt16.1.681&rgn=div5

5. Section 114 of the FACT Act
https://www.ftc.gov/sites/default/files/documents/federal_register_notices/identity-theft-red-flags-and-address-discrepancies-under-fair-and-accurate-credit-transactions-act/060718idtheftredflags.pdf

6. Section 615(e) of the Fair Credit Reporting Act (FCRA)
https://www.consumer.ftc.gov/articles/pdf-0111-fair-credit-reporting-act.pdf

7. VCU Release of Employment and Personal Information
https://policy.vcu.edu/sites/default/files/Maintenance%20and%20Release%20of%20Employment%20and%20Personal%20Information.pdf

8. State Government Data Collection and Dissemination Practices Act, § 2.2-3800
https://vacode.org/2016/2.2/II/B/38/

9. State Policy 6.05, Personnel Records Disclosure
http://web1.dhrm.virginia.gov/itech/hrpolicy/pol6_05.html

10. State Policy 6.10, Personnel Records Management
http://www.dhrm.virginia.gov/docs/default-source/hrpolicy/pol6_10personnelrecordsmanagement.pdf?sfvrsn=2

Revision History

This policy supersedes the following archived policies:

Approval/Revision Date	Title
May 15, 2009	*Identity Theft Prevention*

FAQ

What are examples of "covered accounts" at VCU?

1. Student Installment Payment Plan Accounts
Responsible Office - Student Accounting

2. Student Deferred Payment Plan Accounts
Responsible Office - Student Accounting

3. Student Accounts with Refund Transactions
Responsible Offices - Student Accounting/Treasury Services

4. Student Accounts in Collection with Payment Arrangements
Responsible Office - Treasury Services

5. Loan Accounts
Responsible Offices - Financial Aid/Treasury Services

6. VCUCard Prepaid Declining Stored - Value Accounts
Responsible Offices - Technology Services/Campus Card Services

7. Student Lockbox Payments
Responsible Offices - Student Accounting/Treasury Services

8. Credit Bureau Access
Responsible Office - Treasury Services

9. Payroll Accounts
Responsible Office – Human Resources