Identity Theft Prevention Program

In December 2008 the VSC Board of Trustees recognized that some activities of the VSC are subject to the provisions of the Fair and Accurate Credit Transactions Act (FACT Act) and its "Red Flag" rules.

I. Program Adoption

The VSC has adopted this Identity Theft Prevention Program (Program) in compliance with the

identity theft, changes in identity theft methods; changes in identity theft detection, mitigation and prevention methods; changes in types of accounts the VSC maintains; changes in the VSC's business arrangements with other entities, and any changes in legal requirements in the area of identity theft. After considering these factors, the Program Coordinator will determine whether changes to the Program, including the listing of Red Flags, are warranted. The Program

Red Flag: A pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

V. Identification of Red Flags

In order to identify relevant Red Flags, the VSC considers the types of accounts that it offers and maintains, the methods it provides to open its accounts, the methods it provides to access its accounts, and its previous experiences with Identity Theft. The following are relevant Red Flags, in each of the listed categories, which employees should be aware of and diligent in monitoring for:

A. Notifications and Warnings from Credit Reporting Agencies

- Report of fraud accompanying a credit report;
- Notice or report from a credit agency of a credit freeze on a customer or applicant; Notice or report from a credit agency of an active duty alert for an applicant; and
- Indication from a credit report of activity that is inconsistent with a customer's usual pattern or activity.

B. Suspicious Documents

- Identification document or card that appears to be forged, altered or inauthentic;
- Identification document or card on which a person's photograph or physical description is not consistent with the person presenting the document;
- Other document with information that is not consistent with existing customer information (such as if a person's signature on a check appears forged); and
- Application for service that appears to have been altered or forged.

C. Suspicious Personal Identifying Information

- Identifying information presented that is inconsistent with other information the customer provides (example: inconsistent birth dates);
- Identifying information presented that is inconsistent with other sources of information (for instance, an address not matching an address on a credit report);
- Identifying information presented that is the same as information shown on other applications that were found to be fraudulent;
- Identifying information presented that is consistent with fraudulent activity (such as an invalid phone number or fictitious billing address);
- Social security number presented that is the same as one given by another customer; An address or phone number presented that is the same as that of another person;
- A person fails to provide complete personal identifying information on an application when reminded to do so (however, by law social security numbers must not be required); and
- A person's identifying information is not consistent with the information that is on file for the customer.

D. Suspicious Account Activity or Unusual Use of Account

- Change of address for an account followed by a request to change the account holder's name; Payments stop on an otherwise consistently up-to-date account;
- Account used in a way that is not consistent with prior use (example: very high

VIII. Responding to Red Flags and Mitigating Identity Theft

In the event VSC personnel detect any identified Red Flags, such personnel, in consultation with their supervisor, shall take appropriate steps to respond to and mitigate identity theft depending on the nature and degree of risk posed by the Red Flag, including but not limited to the following examples:

- Continue to monitor an account for evidence of Identity theft;
- Contact the customer;
- Change any passwords or other security devices that permit access to accounts;
- Not open a new account;
- Close an existing account;
- Reopen an account with a new number;
- Notify law enforcement; or
- Determine that no response is warranted under the particular circumstances.

IX.