Veterans Benefits Administration
Department of Veterans Affairs
Washington, DC 20420

Circular 26-18-28
December 13, 2018

Loan Guaranty Red Flag Rules Policy

1. Purpose. This Circular conveys Loan Guaranty Service's Red Flag Rules Policy to aid in the detection, prevention, and mitigation of identity theft in connection with the Department of Veteran Affairs (VA) portfolio loans.

2. Background. In order to implement Sections 114 and 315 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act); Federal financial institution regulatory agencies, National Credit Union Association (NCUA, and Federal Trade Commission (FTC) jointly issued final rules in 2007 requiring financial institutions and creditors to establish written identity theft "red flags" policies and procedures. The FTC rule regarding the detection, prevention, and mitigation of identify theft applies to creditors that are subject to administrative enforcement of the Fair Credit Reporting Act by the FTC, which includes governmental credit grantors such as VA. The rule requires the development and implementation of a written Identity Theft Prevention Program. The mandatory compliance date for the rule was June 1, 2010.

3. Identity Theft Prevention Program. Exhibit A, "Red Flag Rules Policy," contains VA's written identity theft policy and procedures. It governs all instances in which VA is a creditor, including Native American Direct Loans (NADL), refunded VA-guaranteed loans, and vendee loans from the sale of VA-acquired properties.

4. Action. Regional Loan Centers may disseminate VA's Red Flag Policy to all personnel involved in the origination of NADLs and the refunding of VA-guaranteed loans. VA Central Office provides the Red Flag Policy to contractors originating vendee loans and servicing all VA portfolio loans, and ensures that the contractors have established internal policies at least as comprehensive as those developed by VA.

5. Questions. Questions may be directed to Rhonda Armitage at Rhonda.Armitage@va.gov.

6. Rescission: This Circular is rescinded January 1, 2020

By Direction of the Under Secretary for Benefits

Jeffrey F. London
Director, Loan Guaranty Service

Distribution: CO: RPC 2024 SS (26A1) FLD: VBAFS, 1 each (Reproduce and distribute based on RPC 2024)

RED FLAG RULES POLICY

STATEMENT OF PURPOSE

Pursuant to the Federal Trade Commission's (FTC's) Red Flags Rules Policy, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003 16 C.F.R.§ 618.2, the Department of Veteran's Affairs (VA) designed this policy (the "Policy") to aid in the detection, prevention, and mitigation of identity theft in connection with the opening of a Covered Account or an existing Covered Account and to provide for continued administration of this Policy. The Policy and related procedures will demonstrate the following for covered accounts managed by Loan Guaranty Service (LGY):

- Identification and detection of relevant red flags
- Prevention/mitigation of relevant red flags
- Provisions for administration and maintenance of the policy

2. SCOPE

Accounts associated with the following loan types meet the FTC's definition of a "Covered Account" and are thereby included within the scope of this program.

2.1 Vendee Loan program (38 U.S.C. § 3733) - VA directs a nationwide home loan guaranty program for eligible Veterans. When a loan is foreclosed, VA usually acquires and resells the single-family residences and condominiums that were the security for the loans. These acquired properties may be resold to Veterans, non-Veterans, or investors for cash or with VA financing in the form of 30-year fixed-rate mortgage loans. Loans financed by VA are known as "Vendee loans" and are underwritten by the Property Management Contractor using the same guidelines established for VA's Home Loan Guaranty Program. Vendee loans are maintained by the Loan Servicing Contractor as part of VA's national loan portfolio.

2.2 Native American Direct Loan (NADL) program (38 U.S.C. § 3761, et seq.) - VA may make direct loans to Native American Veterans who are members of a Federally-recognized tribe to purchase, construct, or improve a home on Federal trust land. These loans may also be used to simultaneously purchase and improve a home or to refinance another VA NADL in order to lower the interest rate. NADLs are underwritten by VA and are maintained by the Loan Servicing Contractor in VA's national loan portfolio.

2.3 Refunded loans held by VA (38 U.S.C. § 3720 and § 3732) - When a holder of a VA-guaranteed loan determines that loss mitigation options (repayment plan, special forbearance, or modification) for a defaulted Veteran borrower are not feasible, VA has discretionary authority to "refund" (purchase) a loan from the holder by paying the unpaid principal balance, plus accrued interest. The law providing this authority does not vest borrowers with any right to have their loans refunded, nor does it allow borrowers to "apply" for refunding. VA considers whether refunding is in the best interest of the Veteran and VA in every case of default.

3. DEFINITIONS

3.1 The term "Identity Theft" is defined as a fraud committed or attempted using the identifying information of another person without authority.

3.2 The term “Covered Account” (Account) is defined as “(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of financial institution or creditor from identify theft, including financial, operational, compliance, reputation, or litigation risks.”

3.3 Loan Servicing Contractor: The entity delegated authority under 38 C.F.R. § 36.4342(e) and §36.4845(e) to perform loan servicing functions.

3.4 Property Management Contractor: The entity delegated authority under 38 C.F.R. § 36.4342(f) and § 36.4845(f) to perform property management functions.

4. POLICY

4.1 Identification and Detection of Red Flags

VA monitors several categories of warning signs in detecting possible identity theft:

1. Alerts, Notifications, and Warnings from a Credit Reporting Company, which may include:
    a. A fraud or active duty alert on a credit report;
    b. A notice of credit freeze in response to a request for a credit report;
    c. A notice of address discrepancy provided by a credit reporting agency;
    d. A credit report indicating a pattern of activity inconsistent with the person’s history.

2. Suspicious Documents, which may include:
    a. Identification that looks altered or forged;
    b. The person presenting the identification does not look like identification photo;
    c. Information on identification that differs from what the person presenting the identification has presented;
    d. Signature does not match that on identification;
    e. An application or other document (such as a discharge) that looks like it has been altered, forged, or torn up and reassembled.

3. Suspicious Personal Identifying Information, which may include:
    a. Inconsistent information;
    b. Information that has been used on an account already known as fraudulent;
    c. Fictitious address, an address for a mail drop or prison, an invalid phone number, or one that is associated with a pager or answering service;
    d. Social Security number that has been used by someone else;
    e. An address or telephone number used by many other people opening covered accounts;
    f. Omissions of necessary information;
    g. Failure to answer challenge questions.

4. Suspicious Account Activity, which may include:
    a. A new account used in ways associated with fraud;
    b. An account used in a way inconsistent with established patterns;
    c. Activity in an otherwise long inactive account;
    d. Undeliverable mail, despite continued transactions.

5. Notice from Other Sources:
    a. Notice from a lender or other creditor that an account has been opened or used fraudulently;
    b. Notice from a law enforcement that a fraud has possibly been committed;
    c. Notice from another credible source that someone may have committed identity theft.

4.2 Prevention of Identity Theft

VA has established a number of procedures to prevent identity theft.

1. New Covered Accounts: All applicants must provide accurate information and appropriate identification to verify the information provided.
    a. Documents such as a driver's license, Social Security card, or other official documentation are required, as necessary. Depending on the circumstances, VA will compare information provided by an applicant with information from other sources, such as a credit reporting agency, military service records, or other reliable sources to help prevent fraud and identity theft.
    b. Investigate any behavior that indicates the possibility of fraud and identity theft.

2. Existing Covered Accounts: To detect red flags for existing covered accounts, VA will:
    a. Authenticate that those inquiring about a Covered Account are authorized;
    b. Monitor account transactions for suspicious activity;
    c. Ensure that all relevant electronic information meets VA security standards;
    d. Investigate any behavior that indicates the possibility of fraud and identity theft.

4.3 Mitigation of Identity Theft / Responding to Red Flags

In the event LGY or a service provider discovers a red flag for possible incident of fraud or identity theft, the case will be referred to the VA Office of Inspector General for further investigation. A hold will be placed on the subject Covered Account and/or transaction as necessary, and LGY will follow all appropriate VA security-related memoranda on how to manage security breaches.

5. ADMINISTRATION AND OVERSIGHT OF THE POLICY

5.1 The LGY Director is responsible for implementation and administration of the Policy.

5.2 VA will periodically update the Policy to ensure that it keeps current with identity theft risks. Factors to consider include:

5.2.1 Changes to the Covered Accounts;
5.2.2 New methods to detect, prevent, and mitigate identity theft;
5.2.3 Changes in loan programs or contractual service providers;
5.2.4 Lessons learned from any incident of identity theft.

6. OVERSIGHT OF VA SERVICE PROVIDERS

The Director of VA Loan Guaranty Service will ensure at least annually that the Loan Servicing Contractor, the Property Management Contractor, and any other contractual service provider responsible for opening or maintaining Covered Accounts has implemented a Red Flags Rule policy that is at least as comprehensive as the one adopted by VA.