VIRGINIA MILITARY INSTITUTE
Lexington, Virginia

GENERAL ORDER)
NUMBER 58) 28 September 2020

Identity Theft Red Flags Policy

1. **Purpose:** In November 2007, final rules implementing section 114 of the Fair and Accurate Credit Transactions Act of 2003 were issued by the Federal Trade Commission ("FTC"), the federal bank regulatory agencies, and the National Credit Union Administration ("NCUA"). A joint notice of final rulemaking was published in the Federal Register (72 FR 63718) finalizing the *Identity Theft Red Flags Rule* ("the Rule"). The Rule was issued with the underlying goal of detecting, preventing, and mitigating identity theft "in connection with the opening of certain accounts or existing accounts," referred to as "*covered accounts*."

   Red Flags are defined by the Rule as those events that should alert an organization that there is a possible risk of identity theft. The Rule supplements existing legislation aimed at preventing identify theft through tightened data security by addressing situations where individuals are attempting to use another person's identity in order to fraudulently obtain resources or services. Institutions are to identify Red Flags to alert to and intervene against the possibility of such attempts.

   This policy will be implemented in coordination with General Order Number 54 –Privacy Policy. The privacy policy establishes and clarifies how VMI uses and manages personal information provided to or collected by VMI.

2. **VMI as a Covered Entity:** The Rule applies to financial institutions and creditors that offer or maintain accounts that provide for multiple transactions primarily for personal, family, or household purposes. The Rule defined "account" as a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household or business purposes. Account includes: (i) An extension of credit, such as the purchase of property or services involving deferred payment; and (ii) a deposit account."

   VMI is considered a covered entity because we act as a "creditor" by:
   - regularly extending, renewing, or continuing credit; or
   - regularly arranging for the extension, renewal, or continuation of credit; or
   - acting as an assignee of an original creditor who participates in the decision to extend, renew, or continue credit.

   Part 681 of the Fair Credit Reporting Act contains three Sections on Identity Theft Rules (681.1 and 681.2 apply to VMI)
   - *(681.1) Users of consumer reports must develop reasonable policies and procedures to apply when they receive notice of an address discrepancy from a consumer reporting agency.* This provision would only apply to VMI in the area of background checks for new hires as the Institute does not currently utilize consumer reporting agencies for any

other reason; i.e. credit or background checks for loan issuance or collection purposes, etc.

- *(681.2) Financial institutions and creditors holding 'covered accounts' must develop and implement a written Identity Theft Prevention Program designed to detect, prevent and mitigate identity theft in connection with both new and existing accounts.* This provision applies to any areas of VMI that issue any type of credit; i.e. Perkins Loans, administration of Federal Student Loan programs, short term loans for cadets, cadet tuition/fee deferred payment plans, travel advances, etc.
- *(681.3) Debit and credit card issuers must develop policies and procedures to assess the validity of a request for a change of address that is followed closely by a request for an additional or replacement card.* VMI does not directly issue debit or credit cards.

3. **Summary of the Rule Requirements:** Covered entities under the Rule must adopt and implement a written Identity Theft Prevention Program to *detect*, *prevent*, and *mitigate* identity theft in connection with the opening of a covered account, or any existing covered account. The Identity Theft Prevention Program may be integrated into the structure of an existing Compliance Program. However, the efforts and resources committed must be appropriate to the size and complexity of the organization and the nature and scope of its activities. Elements required by the Rule include:
   - Identification of Red Flags – Policies and procedures to identify which Red Flags, singly or in combination, are relevant to detecting the possible risk of identity theft to customers using a risk evaluation method appropriate to the organization.
   - Detection of Red Flags – Policies and procedures designed to prevent and mitigate identity theft in connection with opening an account or any existing account.
   - Responding to Red Flags – Policies and procedures to assess whether the Red Flags detected evidence a risk of identity theft. There must also be a reasonable basis for concluding that a Red Flag does not evidence a risk of identity theft.
   - Updating the Program – Policies and procedures in place to ensure the program is updated periodically to reflect changes in risks to the customer and institution.
   - Administration of the Program – Involvement of senior management in development, implementation and oversight. Ongoing staff training is required. Also included is oversight of service provider arrangements to ensure they are in compliance.

4. **Twenty-Six Red Flags Identified in the Rule:** As an Appendix to the Rule, the FTC identified twenty-six Red Flags that the Institute may consider incorporating into their program. While some of these Red Flags may not apply to current VMI operations, all twenty-six are included for reference purposes. The Red Flags are subdivided into five sections:

   <u>Alerts, Notifications or Warnings from a Consumer Reporting Agency</u>
   - A fraud or credit alert is included with a consumer report.
   - A notice of credit freeze on a consumer report is provided from a consumer reporting agency.
   - A consumer reporting agency provides a notice of address discrepancy.

- A consumer report indicates a pattern of activity inconsistent with the history and usual pattern of activity of a customer.

Suspicious Documents

- Documents provided for identification appear to have been altered or forged.
- The photograph or physical description on the identification is not consistent with the appearance of the customer presenting the identification.
- Other information on the identification is not consistent with information provided by the person opening an account or presenting the identification.
- Other information on the identification is not consistent with readily accessible information that is on file with the Institute.
- An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

- Personal identifying information provided is inconsistent when compared against external information sources used by the Institute.
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.
- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Institute.
- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by the internal or third-party sources used by the Institute.
- The social security number provided is the same as that submitted by other persons opening an account or other customers.
- The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of customers or other persons opening accounts.
- The person opening the account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.
- Personal identifying information provided is not consistent with personal identifying information that is on file with the Institute.
- If the Institute uses a challenge question, the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

- Shortly following the notice of a change of address, the Institute receives a request for a new or replacement card or cell phone, or the addition of authorized users on the account.
- A new revolving credit account is used in a manner commonly associated with known patterns of fraud.
- An account is used in a manner that is not consistent with established patterns of activity on the account.
- An account that has been inactive for a reasonably lengthy period of time is used.

- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the account.
- The Institute is notified that the customer is not receiving paper account statements.
- The Institute is notified of unauthorized charges or transactions in connection with a customer's account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection with Covered Accounts

The Institute is notified by a customer, a victim of identity theft, a law enforcement authority, or any person that it has opened a fraudulent account for a person engaged in identity theft.

5. Policy and Procedures for the Rule:

It shall be the policy of the Institute to:

- Verify identification for any cadet, faculty, or staff member requesting financial related information. The identification should be scrutinized to verify that it has not been altered or forged.
- Ensure that cadets who elect to apply for financial aid complete and submit the Social Security Number Disclosure Waiver to the Admissions office, who then keys related information into Colleague upon receipt and forwards the final cadet admissions packets to the Registrar's office for archiving.
- When a picture ID is requested, verify that the picture on the identification provided matches the appearance of the customer presenting the identification.
- Notify supervisor of noted discrepancies on the identification that is inconsistent with other information on file at the Institute.
- Verify that requests for information updates have not been altered or forged, or that the paperwork gives the appearance of having been destroyed and reassembled.
- Not share student information with anyone other than the cadet unless the cadet has authorized release of information and authorization is documented in Colleague on the STMC screen. Questions regarding FERPA should be directed to the Registrar's Office.
- Address changes for current cadets should be made in person with the Registrar.
- Investigate and verify the correctness of unauthorized charges or transactions assessed by Cadet Accounting in connection with a customer's account. If there are questions regarding the correctness of departmental charges, refer them to the appropriate department for resolution.
- Notify the Comptroller immediately if the Institute is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened, discovered, or manipulated a fraudulent account for a person engaged in identity theft.
- Not provide any information to an individual claiming to be the victim of identity theft without them providing evidence of a Police report or an FTC affidavit of identity theft. If a customer needs assistance of this type, the request must be in writing with detailed information requested as well as proof of positive identification and proof of claim of identity theft (police report or FTC affidavit).
- Ensure that customers who call are not given information on an account if they cannot provide appropriate validating information such as full customer name, SSN, birth date, Colleague ID#, cadet class year, cadet company, cadet rank, and/or other relevant validating information as may be determined by the department. Be cautious about callers who attempt to get financial information without providing any substantive knowledge about the account.

- Ensure that financial and cadet services staff do not respond to any questions from customers related to any medical or counseling services. All calls of this type should be immediately referred to the VMI Health Center.

6. **Oversight, Training, Third Party Compliance and Update:** Due to the sensitive nature of this topic, the supervisor of each applicable area within the Institute will maintain responsibility for the implementation and ongoing support of this regulation. On an annual basis, the supervisor must be ready to verify adherence to the procedures and report compliance to the Comptroller.

   Training on this policy will be conducted annually by the Comptroller's Office at or near the beginning of each academic year. This training is mandatory for all staff with access to customer financial information. If staff members are not able to complete the training due to extenuating circumstances, their supervisors will update them accordingly as soon as practicable.

   Currently there are two Third Party vendors offering debt collection services, which have reported compliance with the FTC Red Flag regulations.

   This policy will be updated as needed based on new processes and procedures.

FOR THE SUPERINTENDENT:

James P. Inman
Colonel, US Army (Ret.)
Chief of Staff

DIST: E
OPR: FAS