RED FLAG RULES COMPLIANCE

INTRODUCTION AND BACKGROUND

On December 4, 2003, The Fair and Accurate Credit Transactions Act ("FACT Act") was signed into law. The FACT Act added several new provisions to 15 U.S.C. § 1681, etc. seq., commonly known as the Fair Credit Reporting Act ("FCRA") and has been actively enforced since January 1, 2011.

Specifically, 15 U.S.C. § 1681m(e) directs the Federal banking agencies, the National Credit Union Administration, the Federal Trade Commission ("FTC"), the Commodity Futures Trading Commission, and the Securities and Exchanges Commission (collectively, the "Agencies") to issue joint regulations and guidelines regarding the detection, prevention, and mitigation of identity theft, including special regulations requiring debit and credit card issuers to validate notifications of changes of address under certain circumstances, as prescribed under 15 U.S.C. § 1681c(h). Section 1681m also provides regulations to establish reasonable policies and procedures for implementing the guidelines ("Identity Theft Prevention Program", "Program", or "ITPP"), to identify possible risks to account holders or customers or to the safety and soundness of the institution or customer. The guidelines must be updated as often as necessary, and cannot be inconsistent with the policies and procedures issued under 31 U.S.C. 5318(l), which was amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, or "USA PATRIOT Act," requiring verification of the identity of persons opening new accounts. The Agencies have also considered reasonable guidelines that would apply when a transaction occurs in connection with a consumer's credit or deposit account that has been inactive for two years. These guidelines provide that in such circumstances, a financial institution or creditor "shall follow reasonable policies and procedures" for notifying the consumer, "in a manner reasonably designed to reduce the likelihood of identity theft."

DEFINITIONS

Employees are expected to understand what a Red Flag is, and how it related to Identity Theft.

Definition of *Red Flag*:

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

Definition of *Identity Theft*:

> "A fraud committed or attempted using the identifying information of another person without authority."

Definition of *Covered Account*:

"A covered account is generally: (1) 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; or (2) any other account that poses a reasonably foreseeable risk to customers of identity theft." [1]

Definition of *Identifying Information* or *Personally Identifiable Information* ("PII"):

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

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; and

3. Unique electronic identification number, address, or routing code."

I. POLICY CONCERNING THE IDENTITY THEFT PREVENTION PROGRAM

Nevada West Financial's policy is to protect our customers and their accounts from identity theft and to comply with the Red Flags Rule pursuant to the FACT Act. We will do this by developing and implementing this written ITPP, which will be appropriate to our size and complexity, as well as the nature and scope of our activities. Our identity theft prevention policies, procedures, and internal controls will be reviewed and updated periodically to ensure they adapt to both changes in the regulatory climate on a state to state level as well as federally, and as they relate specifically to our business.

This ITPP is designed to; 1) identify, 2) detect, 3) respond to, as well as mitigate identity theft, and 4) update policies as needed.

II. IMPLEMENTATION OF GUIDELINES

A program coordinator ("Program Coordinator") will be designated by the Director of Credit and Risk, the Director of Loan Servicing, or directly by the CEO, and will be responsible for reviewing identity theft complaints sent directly to Nevada West Financial, and selecting a sample of credit disputes received throughout the course of the year that have specifically indicated that

[1] https://www.sec.gov/info/smallbus/secg/identity-theft-red-flag-secg.htm

the reason for dispute is identity theft. The Project Coordinator will also review a sample of applications that are returned or rejected due to the inability of the Verifications Department to verify a consumer's information or because they were unable to speak with consumer and complete a new customer interview.

The four basic elements mentioned above are incorporated and included in the Program as follows:

1. Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program;
    a. Risk Factors for identifying relevant red flags are:
        i. Types of covered accounts offered or maintained;
        ii. Methods provided to open or access covered accounts; and
        iii. Previous experiences with identity theft.
    b. Sources of red flags are:
        i. Incidents of identity theft that have been experienced;
        ii. Methods of identity theft reflecting changes in identity theft risks; and
        iii. Applicable supervisory guidance.
    c. Five Categories of red flags are:
        i. Alerts, notifications, or other warnings received from consumer reporting agencies or service providers;
        ii. Presentation of suspicious documents;
        iii. Presentation of suspicious personal identifying information;
        iv. Unusual use of, or other suspicious activity related to a covered account; and
        v. Notice from customers, victims of identity theft, or law enforcement authorities.

2. Detect Red Flags that have been incorporated into the Program;
    a. Verify identify;
    b. Authenticate customers;
    c. Monitor transactions; and
    d. Verify validity of address changes.

3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft;
    a. Monitor accounts;
    b. Contact customer;
    c. Change passwords, or require that a customer re-authenticate their access to their online account;
    d. Close and reopen an account;
    e. Refuse to open an account;
    f. Don't collect on or sell account; or

g. Notify law enforcement.

Finally,

4. Update. Ensure that the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft.

III. THE TWENTY-SIX (26) RED FLAGS

This provision of Title 12 of the Code of Federal Regulations should be used in conjunction with section II to further expand on the four basic elements of the ITPP.

Supplement A of 12 C.F.R. Appendix J to Part 41 [2] provides and defines twenty-six (26) different Red Flags, Nevada West Financial has adopted and selected the relevant Red Flags associated with its business, and they are as follows:

Alerts, Notifications or Warnings from a Consumer Reporting Agency

- A fraud or active duty alert is included with a consumer report.
- A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.
- A consumer reporting agency provides a notice of address discrepancy, as defined in 12 CFR 1022.82(b) of this part.
- A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:
    a. A recent and significant increase in the volume of inquiries;
    b. An unusual number of recently established credit relationships;
    c. A material change in the use of credit, especially with respect to recently established credit relationships; or
    d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

- Documents provided for identification appear to have been altered or forged.

[2] https://www.law.cornell.edu/cfr/text/12/appendix-J_to_part_41

- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

- Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

- 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 financial institution or creditor. For example:
    a. The address does not match any address in the consumer report; or
    b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
    a. The address on an application is the same as the address provided on a fraudulent application; or
    b. The phone number on an application is the same as the number provided on a fraudulent application.

- Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:
    a. The address on an application is fictitious, a mail drop, or a prison; or
    b. The phone number is invalid, or is associated with a pager or answering service.

- The SSN 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 other persons opening accounts or by other customers.

- The person opening the covered account or the customer 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 financial institution or creditor.

- For financial institutions and creditors that use challenge questions, the person opening the covered account or 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 for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

- The financial institution or creditor is notified that the customer is not receiving paper account statements.

Notice From Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

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

IV. MANAGEMENT AND TRAINING

The FTC considers motor vehicle retailers or dealers, and lenders, in the high-risk identity theft category, and believes that as part of their usual and customary business practices, that dealers and lenders already take steps to minimize losses due to fraud. Only relevant staff will need to be trained to implement the Program, as necessary – meaning, for example, that staff already trained as a part of a covered entity's anti-fraud prevention efforts do not need to be retrained except as incrementally needed.

At least annually, the Program Coordinator will report to the Director of Credit and Risk or directly to the CEO regarding:

1. The effectiveness of the Program;

2. Explaining "significant events" involving identity theft and management's response to any incident; and

3. Providing recommendations for substantive or material changes to the Policies and Procedures due to evolving risks and methods of identity theft.

In the event of a positive trend in significant events and/or complaints and disputes directly related to identity theft—at the discretion and direction of the Director of Credit and Risk, the Director or Loan Servicing, or the CEO—training hours may be designated for relevant employees to participate in education programs related to the four basic elements of this ITPP and the twenty-six Red Flags.

V. PROCEDURES FOR OBTAINING CUSTOMER INFORMATION AND VERIFYING CUSTOMER IDENTITY

The following procedures will be implemented with respect to obtaining customer information and verifying customer identities, and may be duplicative of already existing policies and procedures related to the Verifications Department:

Forms are collected and utilized by Nevada West Financial that request customer information, such as names, addresses, telephone numbers, birth dates, social security numbers, tax identification numbers, and driver's license and insurance information, to enable Nevada West Financial to verify the identification of its customers. In addition, customers must sign documentation, including sworn statements in some cases, wherein the customer represents and warrants that he/she is the person identified in the documentation.

Employees will request to see the customer's driver's license or other form of government-issued identification bearing a photograph to verify the customer's identity and will make a copy of the same to retain in the customer's file. If a customer requests financing in connection with a

transaction, the customer will be required to provide employment information and references and must authorize Nevada West Financial to obtain a credit report, all of which may be utilized to verify the identity of the customer and be used to check for any notice of an address discrepancy. Employees may also request copies of the customer's utility bills, bank or credit card statements and paycheck stubs.

In the event that customer information provided is conflicting or cannot be verified upon further inquiry, employees shall request additional documentation evidencing the customer's residence and bearing a photograph or other safeguard (i.e. a social security card, alien identification card, or passport) to enable employees to form a reasonable belief that they know a customer's true identity. When appropriate, employees shall write a summary of the means and results of any measures taken to identify a customer, including the resolution of any discrepancy in the identifying information obtained. Employees will be instructed to notify the Program Coordinator if customer information still cannot be verified, or if the employees have obtained information regarding an address discrepancy that cannot be explained.

Paper and electronic records containing customer information and relevant to Nevada West Financial's identity verification process will be retained by Nevada West Financial in accordance with federal and state record retention requirements. Upon the expiration of the appropriate retention period, any such records will be disposed of in a secure manner in accordance with information security standards.

VI. POLICIES AND PROCEDURES CONCERNING INFORMATION SYSTEMS AND ELECTRONIC RECORDS

The following information security standards will be implemented in order to protect customer information collected and maintained by Nevada West Financial and may be duplicative of Statements of Compliance ("SOCs") provided by third-party vendors, internal Information Technology Department policies, or Building Operations policies and procedures:

Employees will have access only to that customer information which is necessary to complete their designated responsibilities. Employees shall not have access to or be authorized to provide any other unauthorized person access to customer information that is obtained during the course of employment. Requests for customer information that are outside the scope of our ordinary business practices or the scope of an employee's authorization must be directed to the Program Coordinator or other designated individuals (such as senior management; the Director of Credit and Risk, the Director Loan Servicing, or the CEO.) Access to electronic customer information will be password controlled. Every employee with access to the computer or servicing system and electronic records will have a unique password including numbers and letters. Only employees that need to access electronic records will be provided with passwords. All paper and electronic records will be stored in secure locations to which only authorized employees will have access. Any paper records containing customer information must be stored in a deal jacket or

folder. Paper records must be stored in an office, desk, or file cabinet that is locked when unattended. Electronic records will be stored on a secure server that is located in a locked room and is accessible only with a password. Where appropriate, records will be maintained in a fireproof file cabinet and/or at an offsite location. Customers, vendors, and service providers shall not be left unattended in an area with customer records. Backups of the computers and/or server will be made at least once every day, or at more frequent intervals as deemed necessary. At least once each month the backup information will be verified. Backup disks will be stored in a locked file cabinet. Virus protection software has been installed on the computers and new virus updates will be checked at regular intervals. All computer files will be scanned at least once each month, or at more frequent intervals as deemed necessary. Firewalls and security patches from software vendors will be downloaded on a regular basis.

All data will be erased from computers, disks, hard drives, or any other electronic media that contain customer information before disposing of them and, where appropriate, hard drives will be removed and destroyed. Any paper records will be shredded and stored in a secure area until an authorized disposal/recycling service picks it up. Employees will be instructed to log off of all Internet, e-mail and other accounts when they are not being used. Employees will not be permitted to download any software or applications to Nevada West Financial's computers or open e-mail attachments from unknown sources. Electronic records may not be downloaded to a disk or individual computer without explicit authorization from the Program Coordinator. Electronic records will not be stored online and are not accessible from the Internet. If customer information is transmitted electronically over external networks, the information will be encrypted at the time of transmittal. Neither current nor former employees will be permitted to remove any customer information from Nevada West Financial, whether contained in paper records or electronic records, or to disclose our information security standards to any person without authorization from the Program Coordinator.

VII. POLICIES AND PROCEDURES CONCERNING SELECTION AND OVERSIGHT OF SERVICE PROVIDERS AND/OR SPECIFIC VENDORS

In order to protect the customer information Nevada West Financial collects, and to deal with notices of address discrepancies, we will take steps to evaluate and oversee our service providers. The following evaluation criteria will be utilized in selecting service providers: Compatibility and willingness to comply with Nevada West Financial's policies and procedures and the adequacy of the service provider's own policies and procedures. Records to be maintained by the service provider and whether Nevada West will have access to information maintained by the service provider. The service provider's knowledge of regulations that is relevant to the services being provided, including privacy, identity theft, and other consumer protection regulations. Experience and ability to provide the necessary services and supporting technology for current and anticipated needs.

Functionality of any service or system proposed and policies concerning maintaining secure systems, intrusion detection and reporting systems, customer authentication, verification, and authorization, and ability to respond to service disruptions. Service and support that will be provided in terms of maintenance, security, and other service levels. Financial stability of the service provider and reputation with industry groups, trade associations, and other lenders.

Contractual obligations and requirements, such as the term of the contract; prices; software support and maintenance; training of employees; customer service; rights to modify existing services performed under the contract; confidentiality, indemnification, limitation of liability and exit clauses; compliance with applicable regulatory requirements; records to be maintained by the service provider; notification of material changes to services, systems, controls and new service locations; and use of the Nevada West Financial data, equipment, and system and application software. The right of Nevada West Financial to audit the service provider's records, to obtain documentation regarding the resolution of disclosed deficiencies.

Service Providers will be required to agree contractually to be responsible for securing and maintaining the confidentiality of customer information, including agreement to refrain from using or disclosing Nevada West Financial's information, except as necessary to or consistent with providing the contracted services, to protect against unauthorized use or disclosure of customer or Nevada West Financial's information, to comply with applicable privacy and identify theft regulations, and to fully disclose breaches in security resulting in unauthorized access to information that may materially affect Nevada West Financial or its customers and to notify Nevada West Financial to the service provider's corrective action.

Service Providers will be subject to ongoing assessment to evaluate their consistency with selection criteria, performance and financial conditions, and contract compliance.

VIII. CONTINGENCY AND MANAGING SYSTEM FAILURES

The Program Coordinator will implement audit and oversight procedures as he/she deems necessary to detect the improper disclosure or theft of customer information or notices of any address discrepancy and to ensure that employees, independent contractors, and service providers are complying with our Retailer/Lender's Policies and Procedures.

If Nevada West Financial's ITPP is breached, the Program Coordinator will inform the CEO and senior management. The Program Coordinator will take appropriate steps to notify legal counsel, service providers, customers, and the appropriate Law Enforcement Agency of any breach, damage or loss of information and the risks associated with the same and will immediately take measures to limit the effect of the breach, identify the reason for the breach and implement procedures to prevent further breaches.

In the event of a breach, or at any other time as the Program Coordinator deems appropriate, the Program Coordinator may modify or supplement our Policies and Procedures.

To assist in compliance with applicable state and federal regulations, the Program Coordinator will audit Nevada West Financial's Policies and Procedures at least annually to determine if the current system is operating effectively to prevent/detect identity theft and to deal with notice of any address discrepancy. Any modification of the system that the Program Coordinator deems appropriate will be implemented as soon as reasonably possible.

As part of the audit program, Nevada West Financial's personnel will be encouraged to advise the Program Coordinator of any newly identified risks to customers or to the safety of Nevada West Financial regarding identity theft. To the extent of any newly identified risk that is discovered, the Program Coordinator is authorized to take appropriate action to address the risk, including assessment, independently or through third parties, of the severity of this risk, and make modifications of the audit system by written instruction to all necessary personnel or through obtaining outside products or services to alleviate the risk.