# FTC Red Flag Policy.

## Balsam West FiberNet, LLC
## Policy for Compliance with FTC Red Flag S 681.2

On November 9, 2007, The Federal Trade Commission ("FTC"), the federal bank regulatory agencies, and the National Credit Union Administration, published a joint notice of final rulemaking in the Federal Register (72 FR 63718) finalizing the Identity Theft Red Flags regulations and guidelines. This rule, promulgated pursuant to the Fair and Accurate Credit Transactions Act of 2003, requires BalsamWest FiberNET, LLC (BWFN) to develop and implement a written "identity theft prevention program" which provides for the identification, detection, and response to patterns, practices or specific activities – known as "red flags" – that could indicate identity theft.

## Identity Theft Policy

### Section 1: Background

The risk to BalsamWest FiberNET, its employees and customers from data loss and identity theft is of significant concern to BWFN and can be reduced only through the combined efforts of every employee and contractor.

### Section 2: Purpose

BalsamWest FiberNET adopts this sensitive information policy to help protect its customers, employees, contractors and BWFN from damages related to the loss or misuse of sensitive information.

This policy will:

1. Define sensitive information;
2. Describe the physical security of data when it is printed on paper
3. Describe electronic security of data when stored and distributed; and
4. Place BalsamWest FiberNET in compliance with regulations regarding identity theft protection

This policy enables BalsamWest FiberNET to protect existing customers, reducing risk from identity fraud, and minimize potential damage to BWFN from fraudulent new accounts. The program will help BWFN:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
2. Detect risks when they occur in covered accounts;
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and

4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program

## Section 3: Scope

This policy and protection program applies to employees, contractors, consultants, temporary workers and other workers at BalsamWest FiberNET, including all personnel affiliated with third parties.

## Section 4: Policy

**4.A: Sensitive Information Policy**

**4.A.1:** Definition of sensitive information

Sensitive information includes the following items whether stored in electronic or printed format:

**4.A.1.a:** Tax Identification numbers, including

1. Social Security Numbers
2. Business Tax ID numbers
3. Employer Tax ID numbers

**4.A.1.b:** Payroll Information, including, among other information:

1. Paychecks
2. Pay stubs

**4.A.1.c:** Medical information for any employee or customer, including but not limited to:

1. Doctor names and claims
2. Insurance Claims
3. Any personal medical information

**4.A.1.d:** Other personal information belonging to any customer, employee or contractor, examples of which may include but not limited to:

1. Date of Birth
2. Address
3. Phone Numbers
4. Maiden Name
5. Names
6. Customer Names

**4.A.1.e:** BalsamWest FiberNET personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. Furthermore, this section should be read in conjunction with BWFN's CPNI policy and policy concerning Mutual Non-Disclosure. If an Employee is uncertain as to the sensitivity of a particular piece of Information, he/she should contact their supervisor.

**4.A.2: Hard Copy Distribution**

Each employee and contractor performing work for BalsamWest FiberNET will comply with the following policies:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when not in use.
3. Desks, workstations, work areas, printers and fax machines, and common areas will be cleared of all documents containing sensitive information when not in use.
4. When documents containing sensitive information are discarded, they will be shredded.

**4.A.3: Electronic Distribution**

Each employee and contractor performing work for BalsamWest FiberNET will comply with the following policies:

1. Internally, sensitive information may be transmitted using approved BWFN email.
2. Any sensitive information sent externally may be sent only to approved recipients. Additionally, a statement such as this should be included in all emails:

"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

## Section 5: Additional Identity Theft Prevention Program
## If BalsamWest FiberNET maintains certain covered accounts pursuant to federal legislation, BWFN may include the additional program details.

**5.A: Covered Accounts**

A covered account may include any account that involves or is designed to permit BWFN payments or transactions. Every new and existing customer account that meets the following criteria is covered by this program:

1. Any accounts for which there is a reasonably foreseeable risk of identity theft; or
2. Any accounts for which there is a reasonably foreseeable risk to the safety or soundness of BWFN from identity theft, including financial operational, compliance, reputation or litigation risks.

**5.B Red Flags**

**5.B.1:** The following red flags are potential indicators of fraud. Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be verified.

1. Alerts, notifications or warnings from a consumer reporting agency;
2. A fraud or active duty alert included with a customer report.

3. Notice of a credit freeze from a consumer reporting agency in response to a request for a consumer report; or
4. A notice of an address discrepancy from a consumer reporting agency.

**5.B.2:** Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of a customer, such as:

- A recent and significant increase in the volume of inquiries
- An unusual number of recently established credit relationships
- A material change in use of credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

**5.C Suspicious Documents**

**5.C.1:** Documents provided for identification that appear to have been altered or forged.

**5.C.2:** The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

**5.C.3:** Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

**5.C.4:** Other information on the identification is not consistent with readily accessible information that is on file with BWFN, such as signature card or a recent check.

**5.C.5:** An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

**5.D Suspicious personal identifying information**

**5.D.1:** Personal identifying information provided is inconsistent when compared against external information sources used by BWFN. For example:

- The address does not match any address in consumer report;
- The Social Security Number (SSN) or Tax Identification Number (TIN) has not been issued.
- Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer.

**5.D.2:** Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third party sources used by BWFN. For example:

- The address on application is fictitious
- The phone number is invalid or is associated with a pager or answering

Service.

**5.D.3:** The customer or person opening the covered account fails to provide all the required personal identifying information on an application or in response to notification that the application is incomplete.

**5.D.4**: Personal identifying information provided is not consistent with personal identifying information that is on file with BWFN.

**5.E: Unusual use of, or suspicious activity related to, the covered account**

**5.E.1:** BWFN is notified that a customer is not receiving paper account statements.

**5.E.2:** BWFN receives notice from customers, victims of identity theft, a law enforcement authority, or any other persons regarding possible identity theft in connection with covered accounts held by BWFN.

**5.E.3:** BWFN 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.

## Section 6: Responding To Red Flags

**6.A: Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and BWFN from damages and loss.**

**6.A.1:** Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority.

**6.A.2:** The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

**6.B: If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:**

1. Canceling the transaction;
2. Notifying and cooperating with the appropriate law enforcement;
3. Determining the extent of liability of BWFN; and
4. Notifying the actual customer that fraud has been attempted.

## Section 7: Periodic Updates to Plan

**7.A:** At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

**7.B:** Periodic reviews will include an assessment of which accounts are covered by the program.

**7.C:** As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

**7.D:** Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage or liability to BWFN and its customers.

## Section 8: Program Administration

### 8.A: Involvement of Management

1. The Identity Theft Protection Program shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.
2. The Identity Theft Prevention Program is the responsibility of the governing body. Approval of the initial plan must be appropriately documented and maintained.
3. Operational responsibility of the program is designated to the CEO or appropriate assignee.

### 8.B: Staff Training

1. Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to BWFN or its customers.
2. Department managers are responsible for ensuring identity theft training for all requisite employees and contractors.
3. Employees must receive annual training is all elements of this policy.
4. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

### 8.C: Oversight of service provider which may have access to sensitive information

1. It is the responsibility of BWFN to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
2. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.