

Minutes of the April 13, 2009 Meeting of the Board of Selectmen.

Present: Neal Fox, Bill Richards, Joe DeFreitas, Delbert Cloud, Geneva Gaiko, Mary Floyd, Fire Chief Robert Dean, Assistant Chiefs David Aldrighetti and Scott Taylor, and Joe Duncan of the engineering firm Forcier Aldrich & Associates.

The meeting was called to order at 6:00 PM by Chairman Neal Fox, the Board first reviewing and approving the weekly payroll and payables. The Constable's reports of April 1, 2009 and April 5, 2009 were reviewed and placed on file. The minutes of the March 23, 2009 meeting of the Board of Selectmen were approved by motion of Joe DeFreitas, seconded by Bill Richards and unanimously carried. A letter of appreciation for Amy Bergamo's work as Chair of the Town Hall Finance Committee was endorsed by the Board members. Delbert Cloud reported information he had obtained from a local tree specialist regarding the trees along the front of the Main Street Parking Lot, the advice in essence being that the trees are still young and some minor amount of pruning could be done in the summer after both the lindens and the apples have flowered; the trees should be suitable for many more years with a modest amount of attention at certain times. The Board members concurred that the recommended work should be done when the appropriate time arrives.

Chairman Fox then welcomed Joe Duncan of Forcier Aldrich & Associates, the time being 6:15 PM. Mr. Duncan updated the Board on his company's work in designing, permitting, and seeking financing for: a new river crossing for the River Street water main and associated work, metering of the water system, and upgrading of the wastewater pump station adjacent to the River Street Bridge. He has been working diligently to develop the projects, in consort with a number of State of Vermont and federal agencies. However, it is extremely difficult at this time to ascertain how regular funding programs, or new programs dispersing "American Recovery and Reinvestment Act" (ARRA) funding, will be utilized. This standing is not unique to the Town's projects, but reflects the uncertainty everyone is facing given the newness of the ARRA programs and how they will be used and interfaced with customary funding sources. It was left that Mr. Duncan would try to gain answers to the many questions to the extent possible prior to the Board's next meeting on April 27<sup>th</sup>. The Board thanked Mr. Duncan for his efforts on these matters, and he departed at 7:00 PM.

Chairman Fox then took the moment to publicly thank Amy Bergamo for her work as Chair of the Town Hall Finance Committee, and presented her with the previously endorsed letter of appreciation for that work. The subject letter also acknowledged her resignation from that position, her resignation being accepted with deep regret.

Chairman Fox then welcomed Fire Chief Robert Dean and Assistant Chiefs David Aldrighetti and Scott Taylor, they being present to inform the Board of a used first response vehicle which they had recently become aware of, this being offered for sale by the Sharpsburg Fire Department in Maryland. The vehicle has only 7100 miles on it and is offered at a very reasonable price (negotiated down from \$60,000.00 to \$50,000.00). It is equipped very favorably to provide for our Department's needs, and the Chiefs strongly recommended taking action to hold the vehicle until it can be fully inspected by them. The cost to do this would be \$5,000.00, applicable against purchase, and the acquisition would be commensurate with the intent of the equipment fund for which appropriation had been renewed in the 2010 budget. Delbert Cloud advised that he had consulted with lenders and confirmed that funds could be available to acquire the vehicle if it proved to be as good upon inspection as it seems, subject to the Selectboard's concurrence that the amortization would be provided for within future budgets over five years. After due discussion, motion was made by Bill Richards, seconded by Joe DeFreitas and unanimously carried, to procure the truck subject to the Chiefs' inspection of it to their satisfaction. The members of the Department then briefly discussed with the Board various matters associated with the budget and further equipment needs of the Department, and it was agreed that a schedule of those needs would be developed such that necessary budgeting decisions could be made. At 7:40 PM, the members of the Fire Department left, and the Board returned to the order of the agenda.

The Town Hall rehabilitation project was the first item taken up, and Amy Bergamo inquired as to the readiness of the project for bidding. Delbert Cloud advised everyone of the current reviews being done between the architect and the USDA Rural Development Construction Specialist, and of the Town's application for funding now also being reviewed by Rural Development with the hope that favorable financing will be available to the Town through that program, it being the most likely source of American Recovery

and Reinvestment funds, as well. However, it is necessary to have all plans, documents, and procedures approved “up front” by Rural Development. An “offering” of financial assistance is anticipated, but the Town has not yet received it. Given the necessary coordination with Rural Development officials, it should still be possible to bid the project in May, which would be ahead of many other projects now being planned in other locales. The specifications are basically done, subject to a few points about which the Town must make confirmation, hopefully at this evening’s meeting.

Regarding the plans and specifications, the following points were agreed upon: (1) the ductwork for a commercial stove should be installed within all enclosed spaces in compliance with requirements of today’s building codes, and space should be kept in the kitchen lay-out for a six-burner commercial range and at least four linear feet of refrigeration, but neither the stove nor the refrigeration units should be supplied/installed by the contractor, (2) no air conditioning should be called for at this time in the first floor, (3) radiant floor heating should be stated as the first priority for heating the first floor, with baseboard as an alternate, (4) the first floor should be electrified as one open space with perhaps four “zones” and access to the electrical system in each whereby additional circuitry could be added when need required, and (5) the foyer design should be evaluated to make sure the Town is satisfied with the architect’s plan for it to be attractive and suitably inclusive of provision for display of memorabilia, etc.

Mary Floyd suggested names of a few people that she thought were willing to continue to serve on the Town Hall Committee. Amy Bergamo said she believes a committee will need to devote time to constant fund raising to help maintain the building, and to “marketing” the building to make sure it is used and not left sitting idle. It was agreed that an advertisement to seek people interested in working on the committee should be run in the next two issues of the “Herald;” interested people can call Mary Floyd if they have questions, or simply attend the next committee meeting to be at the Bethel Library on April 23<sup>rd</sup> at 7:00 PM.

Delbert Cloud then updated the Board on the status of an application for financial assistance which he has also submitted to Rural Development for replacement of the truck scales at the solid waste facility and developing a water supply at that same facility. It is anticipated that Rural Development will be making an “offering” of financial assistance in the near future.

The Board next made review of the Budget Status Reports for the end of the third quarter of the Town General Fund, the Water Department, the Wastewater Department, and the Solid Waste Program. Within the Town General Fund, it was noted that revenues are favorable with the exception of the reduction by the State of Vermont in financial aid for highways. Although some equipment repairs have caused over-runs, most line items appear to be within parameters of the budget. Delbert Cloud expressed concern that there may be a fairly high level of delinquency in the current year of taxes collected, but efforts at collection of prior year obligations have been quite successful to date.

Regarding the construction season rapidly approaching, Cloud reported that both he and the road Foreman, Robert Hyde, would like to spend as much time as possible cleaning ditches, and removing ledge outcroppings and trees from the ditchlines as time would allow; the emphasis on similar work in the preceding year appeared to have been a highly contributing factor to the Town having suffered only a minor amount of erosion damage despite all the rainfall which occurred in 2008. It is also planned that around five thousand yards of gravel will be processed with a contracted crusher at the recently opened pit on Sand Hill Road, with around two thousand yards being stock-piled at the Town Garage for use in the 2010 mud season. Emphasis will also be placed on training for all Town crew members, including use of the grader such that regular work and emergencies can be effectively addressed under most circumstances.

Delbert Cloud reported on his discussion(s) with various people re. an appointment to fill the existing vacancy on the Board of Auditors. With the understanding that Barbara Stearns is willing to accept such appointment, motion accordingly was made by Neal Fox, seconded by Bill Richards and unanimously carried, to appoint Barbara Stearns to the Board of Auditors until such time as an election can be held.

In addition to minor associated editing changes, a new “Section 4” was considered as an amendment to the Town’s “Ordinance for the Control of Dogs.” The previous section numbered as “4” would become number “5” with subsequent re-numbering accordingly

of the remaining existing sections. The proposed addition by amendment addresses the control of “Nuisance Animals,” viz:

“No owner, keeper or other person having control shall permit an animal to be a nuisance animal. For the purposes of this section, nuisance animal means any animal or animals which:

- a. Barks, whines, howls, cries, or makes a noise commonly made by such animals in an excessive and continuous fashion so as to disturb the peace and quiet of any other person.
- b. Defecates off the premises of the animal’s owner, and the owner, or other individual in control of the animal, fails to remove such deposit immediately.”

After due consideration, motion to adopt the proposed amendment, to be effective in the statutorily prescribed sixty days, was made by Neal Fox, seconded by Bill Richards and unanimously carried.

An amendment was then considered of the “Cemetery Rules and Regulations,” specifically to change the wording of Section III – F to read: “No artificial flowers shall be placed on a lot in any Town cemetery.” After due consideration of this matter, the motion to amend the “Cemetery Rules and Regulations” as proposed was made by Neal Fox, seconded by Joe DeFreitas and unanimously carried.

The Vermont League of Cities and Towns has advised that federal regulations require certain Towns and Municipal Departments to adopt an “Identity Theft Prevention Policy” by May 1, 2009. By relative authority as the Legislative Body, The Board of Water Commissioners, and the Board of Sewage Disposal Commissioners, the following policies were adopted by motion of Bill Richards, seconded by Joe DeFreitas and unanimously carried:

#### **“Section 1: Title, Authority, and Purpose**

This policy shall be known as the “Town of Bethel Identity Theft Prevention Policy.” It has been adopted by the Town of Bethel Selectboard pursuant to 24 V.S.A. §§ 872, 1121 and 1122.

The purpose of this Policy is to establish an Identity Theft Prevention Program (“Program”) designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair Accurate Credit Transactions Act (FACTA) of 2003.

#### **Section 2: Definitions**

For the purposes of this Policy, the following definitions apply:

**Covered Account** means:

- an account that a creditor offers or maintains – primarily for personal, family, or household purposes – that involves or is designed to permit multiple payments or transactions, such as an utility account; and
- any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

**Credit** means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.

**Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Creditor includes any municipal utility (water, sewer, electric, etc.).

**Customer** means a person that has a covered account with a creditor.

**Department Personnel** means all employees responsible for or involved in the process of opening a covered account, restoring a covered account, or accepting payment for a covered account.

**Identity theft** means a fraud committed or attempted using the identifying information of another person without authority.

**Person** means a natural person, a corporation, government or governmental subdivision, or agency, trust, estate, partnership, cooperative, or association.

**Personal Identifying Information** means a person’s credit card account information, debit card information, bank account information, and driver’s license information, and for a natural person includes his or her social security number, mother’s birth name, and date of birth.

**Red flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

### **Section 3: Identification of Relevant Red Flags**

In order to identify relevant red flags, the Legislative Body 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 Legislative Body identifies the following examples of relevant red flags, in each of the listed categories:

- **Alerts, Notifications, or Warnings from Consumer Reporting Agencies**
  - A fraud or active duty alert that is included with a consumer report.
  - A notice of credit freeze in response to a request for a consumer report.
  - A notice of address discrepancy provided by a consumer reporting agency.
  - A consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or 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 the 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.
  
- **Suspicious Documents**
  - Documents provided for identification that appear to have been altered or forged.
  - Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer presenting the identification.
  - Other information on the identification that is inconsistent with information provided by the person opening a new covered account or a customer presenting the information.
  - Other information on the identification that is inconsistent with readily accessible information that is on file with the department, such as a signature card or a recent check.
  - An application that appears to have been altered, forged, destroyed, or reassembled.
  
- **Suspicious Personal Identifying Information**
  - Personal identifying information presented that is inconsistent with external information sources used by the department. For example:
    - The address does not match any address in the consumer reports; or
    - The Social Security Number (SSN) has not been issued or is listed on the Social Security Administrator's Death Master File.
  - Personal identifying information provided by the customer is inconsistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth.
  - Personal identifying information or a phone number or address is associated with known fraudulent activities as indicated by internal or third-party sources used by the department.
  - Personal identifying information, such as a fictitious mailing address, mail drop address, jail address, invalid phone number, pager number, or answering service, is associated with fraudulent activities as indicated by internal or third-party sources used by the creditor.
  - The SSN provided is the same as that submitted by another applicant or customer.
  - The address or telephone number provided is the same as or similar to the covered account number or telephone number submitted by an unusually large number of applicants or customers.
  - The applicant or customer fails to provide all required personal identifying information on an application or in response to the notification that the application is incomplete.
  - Personal identifying information is inconsistent with personal identifying information on file with the department.
  - The applicant or 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 department receives a request for 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. For example:
    - The customer fails to make the first payment, or makes an initial payment but no subsequent payments.
  - A covered account is used in a manner inconsistent with established patterns of activity on the account. For example:
    - Nonpayment when there is no history of late or missed payments, or
    - A material increase in the use of available credit.
  - A covered 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 customer's covered account.
  - The department is notified that the customer is not receiving paper account statements.
  - The department is notified of unauthorized charges or transactions in connection with the 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 Held by the Creditor.**
  - The department is notified by a customer, a victim of identity theft, law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

#### Section 4: Detecting Red Flags

- **New Covered Accounts**

In order to detect any of the red flags identified above associated with the opening of a new covered account, department personnel will take the following steps to obtain and verify the identity of the person opening the account:

- Require submission of all of the following identifying information from the customer prior to opening a covered account:
  - name;
  - date of birth;
  - address, which shall be:
    - for an individual, a residential or business street address;
    - for an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business address of a next of kin of another contact individual;
    - for an entity, a principal place of business, local office or other physical address;
    - for a U.S. person, a taxpayer identification number;
    - for a non-U.S. person, one or more of the following:
      - a taxpayer identification number;
      - passport number and country of issuance;
      - alien identification card number; or
      - number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.
- Verify the customer's identity (for instance, review a driver's license or other identification card);
- Review documentation showing the existence of a business entity; and
- Independently contact the customer.

- **Existing Accounts**

In order to detect any of the red flags identified above for an existing covered account, department personnel will take the following steps to monitor transactions with an account:

- Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email, etc.);
- Monitor transactions;
- Verify the validity of change of address requests and other account information requests including information provided for billing and payment purposes.

#### Section 5: Preventing and Mitigating Identity Theft

If department personnel detect any identified red flags, such personnel, after consultation with his/her program administrator, shall take one or more of the following appropriate responses commensurate with the degree of risk posed by the red flag in order to further prevent the likelihood of identity theft occurring with respect to covered accounts:

- Continuing to monitor a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to covered accounts;
- Not opening a new covered account;
- Closing an existing covered account;
- Reopening a covered account with a new account number;
- Not attempting to collect on a covered account;
- Not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

#### Section 6: Program Updates

The Legislative Body shall annually review and, as it deems necessary, update this program along with any relevant red flags to reflect changes in risks to customers or to the safety and soundness of the department from identity theft based on the following factors:

- The department's experiences with identity theft;
- Changes in methods of identity theft;
- Changes in identity theft detection, prevention, and mitigation methods;
- Changes in the types of accounts that the department offers or maintains; and
- Changes in the department's business arrangements with other entities.

#### Section 7: Program Administration

- **Oversight:** The Legislative Body shall be responsible for the oversight of the program including program implementation, reviewing reports prepared by staff regarding the detection, prevention, and mitigation of identity theft in connection with the opening of a covered account or an existing covered account, and approving material changes to the program as necessary to address changing identity theft risks.
- **Staff Reports:** Department staff responsible for implementing the program shall report to the Legislative Body annually on compliance with red flag requirements. The report will address material matters related to the program and evaluate issues such as:
  - The effectiveness of the policies and procedures of the department in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;

- Service provider arrangements;
  - Significant incidents involving identity theft and management’s response; and
  - Recommendations for material changes to the program.
- **Staff Training:** The Legislative Body or its authorized representative will train staff responsible for effectively implementing the program as necessary.
  - **Oversight of Service Provider Arrangements:** If the Legislative Body engages a service provider to perform an activity in connection with one or more covered accounts, the Legislative Body will review such arrangements in order to ensure that the service provider’s activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.”

**“Section 1: Title, Authority, and Purpose**

This policy shall be known as the “Town of Bethel Identity Theft Prevention Policy.” It has been adopted by the Town of Bethel Board of Sewage Disposal Commissioners pursuant to 24 V.S.A. § 3616(a).

The purpose of this Policy is to establish an Identity Theft Prevention Program (“Program”) designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair Accurate Credit Transactions Act (FACTA) of 2003.

**Section 2: Definitions**

For the purposes of this Policy, the following definitions apply:

**Covered Account** means:

- an account that a creditor offers or maintains – primarily for personal, family, or household purposes – that involves or is designed to permit multiple payments or transactions, such as an utility account; and
- any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

**Credit** means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.

**Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Creditor includes any municipal utility (water, sewer, electric, etc.).

**Customer** means a person that has a covered account with a creditor.

**Department Personnel** means all employees responsible for or involved in the process of opening a covered account, restoring a covered account, or accepting payment for a covered account.

**Identity theft** means a fraud committed or attempted using the identifying information of another person without authority.

**Person** means a natural person, a corporation, government or governmental subdivision, or agency, trust, estate, partnership, cooperative, or association.

**Personal Identifying Information** means a person’s credit card account information, debit card information, bank account information, and driver’s license information, and for a natural person includes his or her social security number, mother’s birth name, and date of birth.

**Red flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

**Section 3: Identification of Relevant Red Flags**

In order to identify relevant red flags, the Board of Sewage Disposal Commissioners 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. Board of Sewage Disposal Commissioners identifies the following examples of relevant red flags, in each of the listed categories:

- **Alerts, Notifications, or Warnings from Consumer Reporting Agencies**
  - A fraud or active duty alert that is included with a consumer report.
  - A notice of credit freeze in response to a request for a consumer report.
  - A notice of address discrepancy provided by a consumer reporting agency.
  - A consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or 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 the 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.
- **Suspicious Documents**
  - Documents provided for identification that appear to have been altered or forged.
  - Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer presenting the identification.
  - Other information on the identification that is inconsistent with information provided by the person opening a new covered account or a customer presenting the information.

- Other information on the identification that is inconsistent with readily accessible information that is on file with the department, such as a signature card or a recent check.
  - An application that appears to have been altered, forged, destroyed, or reassembled.
- **Suspicious Personal Identifying Information**
    - Personal identifying information presented that is inconsistent with external information sources used by the department. For example:
      - The address does not match any address in the consumer reports; or
      - The Social Security Number (SSN) has not been issued or is listed on the Social Security Administrator's Death Master File.
    - Personal identifying information provided by the customer is inconsistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth.
    - Personal identifying information or a phone number or address is associated with known fraudulent activities as indicated by internal or third-party sources used by the department.
    - Personal identifying information, such as a fictitious mailing address, mail drop address, jail address, invalid phone number, pager number, or answering service, is associated with fraudulent activities as indicated by internal or third-party sources used by the creditor.
    - The SSN provided is the same as that submitted by another applicant or customer.
    - The address or telephone number provided is the same as or similar to the covered account number or telephone number submitted by an unusually large number of applicants or customers.
    - The applicant or customer fails to provide all required personal identifying information on an application or in response to the notification that the application is incomplete.
    - Personal identifying information is inconsistent with personal identifying information on file with the department.
    - The applicant or 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 department receives a request for 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. For example:
      - The customer fails to make the first payment, or makes an initial payment but no subsequent payments.
    - A covered account is used in a manner inconsistent with established patterns of activity on the account. For example:
      - Nonpayment when there is no history of late or missed payments, or
      - A material increase in the use of available credit.
    - A covered 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 customer's covered account.
    - The department is notified that the customer is not receiving paper account statements.
    - The department is notified of unauthorized charges or transactions in connection with the 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 Held by the Creditor.**
    - The department is notified by a customer, a victim of identity theft, law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

#### **Section 4: Detecting Red Flags**

- **New Covered Accounts**

In order to detect any of the red flags identified above associated with the opening of a new covered account, department personnel will take the following steps to obtain and verify the identity of the person opening the account:

  - Require submission of all of the following identifying information from the customer prior to opening a covered account:
    - name;
    - date of birth;
    - address, which shall be:
      - for an individual, a residential or business street address;
      - for an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business address of a next of kin of another contact individual;
      - for an entity, a principal place of business, local office or other physical address;
      - for a U.S. person, a taxpayer identification number;
      - for a non-U.S. person, one or more of the following:
        - a taxpayer identification number;
        - passport number and country of issuance;
        - alien identification card number; or
        - number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.
  - Verify the customer's identity (for instance, review a driver's license or other identification card);
  - Review documentation showing the existence of a business entity; and
  - Independently contact the customer.

- **Existing Accounts**

In order to detect any of the red flags identified above for an existing covered account, department personnel will take the following steps to monitor transactions with an account:

- Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email, etc.);
- Monitor transactions;
- Verify the validity of change of address requests and other account information requests including information provided for billing and payment purposes.

### **Section 5: Preventing and Mitigating Identity Theft**

If department personnel detect any identified red flags, such personnel, after consultation with his/her program administrator, shall take one or more of the following appropriate responses commensurate with the degree of risk posed by the red flag in order to further prevent the likelihood of identity theft occurring with respect to covered accounts:

- Continuing to monitor a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to covered accounts;
- Not opening a new covered account;
- Closing an existing covered account;
- Reopening a covered account with a new account number;
- Not attempting to collect on a covered account;
- Not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

### **Section 6: Program Updates**

The Board of Sewage Disposal Commissioners shall annually review and, as it deems necessary, update this program along with any relevant red flags to reflect changes in risks to customers or to the safety and soundness of the department from identity theft based on the following factors:

- The department's experiences with identity theft;
- Changes in methods of identity theft;
- Changes in identity theft detection, prevention, and mitigation methods;
- Changes in the types of accounts that the department offers or maintains; and
- Changes in the department's business arrangements with other entities.

### **Section 7: Program Administration**

- **Oversight:** The Board of Sewage Disposal Commissioners shall be responsible for the oversight of the program including program implementation, reviewing reports prepared by staff regarding the detection, prevention, and mitigation of identity theft in connection with the opening of a covered account or an existing covered account, and approving material changes to the program as necessary to address changing identity theft risks.
- **Staff Reports:** Department staff responsible for implementing the program shall report to the Board of Sewage Disposal Commissioners annually on compliance with red flag requirements. The report will address material matters related to the program and evaluate issues such as:
  - The effectiveness of the policies and procedures of the department in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
  - Service provider arrangements;
  - Significant incidents involving identity theft and management's response; and
  - Recommendations for material changes to the program.
- **Staff Training:** The Board of Sewage Disposal Commissioners or its authorized representative will train staff responsible for effectively implementing the program as necessary.
- **Oversight of Service Provider Arrangements:** If the Board of Sewage Disposal Commissioners engages a service provider to perform an activity in connection with one or more covered accounts, the Board of Sewage Disposal Commissioners will review such arrangements in order to ensure that the service provider's activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft."

### **“Section 1: Title, Authority, and Purpose**

This policy shall be known as the “Town of Bethel Identity Theft Prevention Policy.” It has been adopted by the Town of Bethel Board of Water Commissioners pursuant to 24 V.S.A. § 3313(a).

The purpose of this Policy is to establish an Identity Theft Prevention Program (“Program”) designed to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or an existing covered account and to provide for continued administration of the Program in compliance with Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of the Fair Accurate Credit Transactions Act (FACTA) of 2003.

### **Section 2: Definitions**

For the purposes of this Policy, the following definitions apply:

**Covered Account** means:

- an account that a creditor offers or maintains – primarily for personal, family, or household purposes – that involves or is designed to permit multiple payments or transactions, such as an utility account; and
- any other account that the creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks.

**Credit** means the right granted by a creditor to a debtor to defer payment of debt or to incur debts and defer its payment or to purchase property or services and defer payment therefor.

**Creditor** means any person who regularly extends, renews, or continues credit; any person who regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who participates in the decision to extend, renew, or continue credit. Creditor includes any municipal utility (water, sewer, electric, etc.).

**Customer** means a person that has a covered account with a creditor.

**Department Personnel** means all employees responsible for or involved in the process of opening a covered account, restoring a covered account, or accepting payment for a covered account.

**Identity theft** means a fraud committed or attempted using the identifying information of another person without authority.

**Person** means a natural person, a corporation, government or governmental subdivision, or agency, trust, estate, partnership, cooperative, or association.

**Personal Identifying Information** means a person's credit card account information, debit card information, bank account information, and driver's license information, and for a natural person includes his or her social security number, mother's birth name, and date of birth.

**Red flag** means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

### **Section 3: Identification of Relevant Red Flags**

In order to identify relevant red flags, the Board of Water Commissioners 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 Board of Water Commissioners identifies the following examples of relevant red flags, in each of the listed categories:

- **Alerts, Notifications, or Warnings from Consumer Reporting Agencies**
  - A fraud or active duty alert that is included with a consumer report.
  - A notice of credit freeze in response to a request for a consumer report.
  - A notice of address discrepancy provided by a consumer reporting agency.
  - A consumer report indicating a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or 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 the 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.
- **Suspicious Documents**
  - Documents provided for identification that appear to have been altered or forged.
  - Identification on which the photograph or physical description is inconsistent with the appearance of the applicant or customer presenting the identification.
  - Other information on the identification that is inconsistent with information provided by the person opening a new covered account or a customer presenting the information.
  - Other information on the identification that is inconsistent with readily accessible information that is on file with the department, such as a signature card or a recent check.
  - An application that appears to have been altered, forged, destroyed, or reassembled.
- **Suspicious Personal Identifying Information**
  - Personal identifying information presented that is inconsistent with external information sources used by the department. For example:
    - The address does not match any address in the consumer reports; or
    - The Social Security Number (SSN) has not been issued or is listed on the Social Security Administrator's Death Master File.
  - Personal identifying information provided by the customer is inconsistent with other personal identifying information provided by the customer, such as a lack of correlation between the SSN range and date of birth.
  - Personal identifying information or a phone number or address is associated with known fraudulent activities as indicated by internal or third-party sources used by the department.
  - Personal identifying information, such as a fictitious mailing address, mail drop address, jail address, invalid phone number, pager number, or answering service, is associated with fraudulent activities as indicated by internal or third-party sources used by the creditor.
  - The SSN provided is the same as that submitted by another applicant or customer.
  - The address or telephone number provided is the same as or similar to the covered account number or telephone number submitted by an unusually large number of applicants or customers.
  - The applicant or customer fails to provide all required personal identifying information on an application or in response to the notification that the application is incomplete.
  - Personal identifying information is inconsistent with personal identifying information on file with the department.
  - The applicant or 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 department receives a request for 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. For example:
    - The customer fails to make the first payment, or makes an initial payment but no subsequent payments.
  - A covered account is used in a manner inconsistent with established patterns of activity on the account. For example:
    - Nonpayment when there is no history of late or missed payments, or
    - A material increase in the use of available credit.
  - A covered 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 customer's covered account.
  - The department is notified that the customer is not receiving paper account statements.
  - The department is notified of unauthorized charges or transactions in connection with the 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 Held by the Creditor.**
  - The department is notified by a customer, a victim of identity theft, law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

#### **Section 4: Detecting Red Flags**

- **New Covered Accounts**  
In order to detect any of the red flags identified above associated with the opening of a new covered account, department personnel will take the following steps to obtain and verify the identity of the person opening the account:
  - Require submission of all of the following identifying information from the customer prior to opening a covered account:
    - name;
    - date of birth;
    - address, which shall be:
      - for an individual, a residential or business street address;
      - for an individual who does not have a residential or business street address, an Army Post Office (APO) or Fleet Post Office (FPO) box number, or the residential or business address of a next of kin of another contact individual;
      - for an entity, a principal place of business, local office or other physical address;
      - for a U.S. person, a taxpayer identification number;
      - for a non-U.S. person, one or more of the following:
        - a taxpayer identification number;
        - passport number and country of issuance;
        - alien identification card number; or
        - number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.
    - Verify the customer's identity (for instance, review a driver's license or other identification card);
    - Review documentation showing the existence of a business entity; and
    - Independently contact the customer.
- **Existing Accounts**  
In order to detect any of the red flags identified above for an existing covered account, department personnel will take the following steps to monitor transactions with an account:
  - Verify the identification of customers if they request information (in person, via telephone, via facsimile, via email, etc.);
  - Monitor transactions;
  - Verify the validity of change of address requests and other account information requests including information provided for billing and payment purposes.

#### **Section 5: Preventing and Mitigating Identity Theft**

If department personnel detect any identified red flags, such personnel, after consultation with his/her program administrator, shall take one or more of the following appropriate responses commensurate with the degree of risk posed by the red flag in order to further prevent the likelihood of identity theft occurring with respect to covered accounts:

- Continuing to monitor a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to covered accounts;
- Not opening a new covered account;
- Closing an existing covered account;
- Reopening a covered account with a new account number;
- Not attempting to collect on a covered account;
- Not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

## Section 6: Program Updates

The Board of Water Commissioners shall annually review and, as it deems necessary, update this program along with any relevant red flags to reflect changes in risks to customers or to the safety and soundness of the department from identity theft based on the following factors:

- The department's experiences with identity theft;
- Changes in methods of identity theft;
- Changes in identity theft detection, prevention, and mitigation methods;
- Changes in the types of accounts that the department offers or maintains; and
- Changes in the department's business arrangements with other entities.

## Section 7: Program Administration

- **Oversight:** The Board of Water Commissioners shall be responsible for the oversight of the program including program implementation, reviewing reports prepared by staff regarding the detection, prevention, and mitigation of identity theft in connection with the opening of a covered account or an existing covered account, and approving material changes to the program as necessary to address changing identity theft risks.
- **Staff Reports:** Department staff responsible for implementing the program shall report to the Board of Water Commissioners annually on compliance with red flag requirements. The report will address material matters related to the program and evaluate issues such as:
  - The effectiveness of the policies and procedures of the department in addressing the risk of identity theft in connection with the opening of covered accounts and with respect to existing covered accounts;
  - Service provider arrangements;
  - Significant incidents involving identity theft and management's response; and
  - Recommendations for material changes to the program.
- **Staff Training:** The Board of Water Commissioners or its authorized representative will train staff responsible for effectively implementing the program as necessary.
- **Oversight of Service Provider Arrangements:** If the Board of Water Commissioners engages a service provider to perform an activity in connection with one or more covered accounts, the Board of Water Commissioners will review such arrangements in order to ensure that the service provider's activities are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft."

With no further business to attend, the motion to adjourn was made at 10:50 PM by Bill Richards, seconded by Joe DeFreitas and unanimously carried.

---

Neal Fox

---

Bill Richards

---

Joe DeFreitas