

MEETING CALLED TO ORDER AT 7:00 PM WITH PLEDGE OF ALLEGIANCE

TRUSTEES ANSWERING ROLL CALL:

ROLL CALL: L. BROOME, HERE; J. PREBISH, HERE; E. KERR, HERE.

**MOTION TO SUSPEND THE REGULAR AGENDA**

MOTION TO SUSPEND THE REGULAR AGENDA BY JEFF PREBISH,  
SECONDED BY LENNY BROOME, ROLL CALL: ALL AYES.

**ROGUES HOLLOW HISTORICAL SOCIETY PARK OPEN FOR THE WINTER**

WILL TRY LEAVING THE PARK IN THE HOLLOW OPEN FOR THE WINTER,  
WE ARE TRYING IT FOR THIS YEAR AND SEE HOW IT GOES.

**08-0144-10 INSURANCE PLAN FOR FULL TIME EMPLOYEES**

RESOLUTION TO OFFER ONLY ONE THE FIRST PPO HEALTH PLAN  
INSURANCE FOR THE EMPLOYEES OF THE TOWNSHIP WHO ARE ELIGIBLE  
FOR THE BENEFITS, MAKING EACH EMPLOYEE COMPLETE THE HEALTH  
ASSESSMENT SURVEY ON LINE BY DECEMBER 1<sup>ST</sup>. MOTION BY LENNY  
BROOME, SECONDED BY LENNY BROOME, ROLL CALL: ALL AYES.

**08-0145-10 ADOPT AN IDENTITY THEFT POLICY**

**A RESOLUTION ADOPTING AN IDENTITY THEFT POLICY**

MOTION BY LENNY BROOME, SECONDED BY JEFF PREBISH,  
WHEREAS, The Fair and Accurate Credit Transactions Act of  
2003, an amendment to the Fair Credit Reporting Act,  
required rules regarding identity theft protection to be  
promulgated; and  
WHEREAS, Those rules become effective November 1, 2008, and  
require local governments to implement an identity theft  
program and policy, and  
WHEREAS, The Chippewa Township Board of Trustees has  
determined that the following policy is in the best interest  
of the Township and its citizens.  
NOW, THEREFORE, BE IT RESOLVED by the Chippewa Township  
Board of Trustees that the following is hereby approved:

**IDENTITY THEFT POLICY**

**SECTION 1: BACKGROUND**

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

**SECTION 2: PURPOSE**

The Township adopts this sensitive information policy to  
help protect employees, customers, contractors and the  
Township 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 the electronic security of data when stored  
and distributed; and
4. Place the Township in compliance with state and  
federal law regarding identity theft protection.

**08-0145-10 ADOPT AN IDENTITY THEFT POLICY (CONTINUED)**

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

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 the Township 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:** Credit card information, including any of the following:

1. Credit card number (in part or whole)
2. Credit card expiration date
3. Cardholder name
4. Cardholder address

**4.A.1.b:** Tax identification numbers, including:

1. Social Security number
2. Business identification number
3. Employer identification numbers

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

1. Paychecks
2. Pay stubs

**4.A.1.d:** Cafeteria plan check requests and associated paperwork

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

**08-0145-10 ADOPT AN IDENTITY THEFT POLICY (CONTINUED)**

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personnel medical information

**4.A.1.f:** Other personal information belonging to any customer; employee or contractor, examples of which include:

1. Date of birth
2. Address
3. Phone numbers
4. Maiden name
5. Names
6. Customer number

**4.A.1.g:** Township 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 the Ohio Public Records Act and the Township's open records policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor. In the event that the Township cannot resolve a conflict between this policy and the Ohio Public Records Act, the Township will contact the Township Law Director.

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

Each employee and contractor performing work for the Township 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 unsupervised.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
5. When documents containing sensitive information are discarded, they will be placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD)-approved shredding device. Locked shred bins are labeled "*Confidential paper shredding and recycling.*" Township records,

**08-0145-10 ADOPT AN IDENTITY THEFT POLICY (CONTINUED)**

however, may only be destroyed in accordance with the Township's records retention policy.

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

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

1. Internally, sensitive information may be transmitted using approved Township e-mail. All sensitive information must be encrypted when stored in an electronic format.

2. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail:

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

**SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION PROGRAM**

**5.A: Covered accounts**

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

1. Business, personal and household accounts for which there is a reasonably foreseeable risk of identity theft; or

2. Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of the Township from identity theft, including financial, operational, compliance, reputation, 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 investigated for verification.

1. Alerts, notifications or warnings from a consumer reporting agency;

2. A fraud or active duty alert included with a consumer report;

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

4. A notice of address discrepancy from a consumer reporting agency as defined in § 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

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

**08-0145-10 ADOPT AN IDENTITY THEFT POLICY (CONTINUED)**

- 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.

**5.C: Suspicious documents**

**5.C.1:** Documents provide 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.

**5C.4:** Other information on the identification is not consistent with readily accessible information that is on file with the Township, such as a 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 the Township. For example:

- The address does not match any address in the consumer report;
- The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or
- Personnel 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.

**5.D.2:** Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the Township. For example, the address on an application is the same as the address provided on a prior fraudulent application.

**08-0145-10 ADOPT AN IDENTITY THEFT POLICY (CONTINUED)**

**5.D.3:** Personnel identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the Township. For example:

- The address on an application is fictitious, a mail drop, or a prison; or
- The phone number is invalid or is associated with a pager or answering service.

**5.D.4:** The SSN provided is that same as that submitted by other persons opening an account or other customers.

**5.D.5:** 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 customers or other persons opening accounts.

**5.D.6:** The customer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

**5.D.7:** Personal identifying information provided is not consistent with personal identifying information that is on file with the Township.

**5.D.8:** When using security questions (mother's maiden name, pet's name, etc.), 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.

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

**5.E.1:** Shortly following the notice of a change of address for a covered account, the Township receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

**5.E.2:** A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments

**5.E.3:** A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

- Nonpayment when there is no history of late or missed payments;
- A material change in purchasing or usage patterns

**5.E.4:** A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

**08-0145-10 ADOPT AN IDENTITY THEFT POLICY (CONTINUED)**

**5.E.5:** Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

**5.E.6:** The Township is notified that the customer is not receiving paper account statements.

**5.E.7:** The Township is notified of unauthorized charges or transactions in connection with a customer's covered account.

**5.E.8:** The Township receives notice from customers, victims or identity theft, law enforcement authorities, or other persons regarding possible identity theft in collection with covered accounts held by the Township.

**5.E.9:** The Township 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 the Township 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 for determination.

**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 Wayne County Sheriff and other appropriate law enforcement;
3. Determining the extent of liability of the Township; 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.

**08-0145-10 ADOPT AN IDENTITY THEFT POLICY (CONTINUED)**

**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 to the Township and its customers.

**SECTION 8: PROGRAM ADMINISTRATION**

**8.A: Involvement of management**

1. The Identity Theft Prevention 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 delegated to Laretta Farlow, Fiscal Officer.

**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 the Township or its customers.

2. Laretta Farlow, Fiscal Officer, is responsible for ensuring identity theft training for all requisite employees and contractors.

3. Employees must receive annual training in 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 or service provider arrangements**

1. It is the responsibility of the Township 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.

CHIPPEWA TOWNSHIP TRUSTEES SPECIAL

TOWNSHIP HALL

7:00 PM

OCTOBER 27,

08

**08-0145-10 ADOPT AN IDENTITY THEFT POLICY (CONTINUED)**

This resolution will take effect immediately upon its passage, the public welfare requiring it.

Upon roll call on the adoption of the Resolution, the vote was as follows:

Lenny Broome, yes; Jeff Prebish, yes; Earl Kerr, yes

**08-0146-10 EXTEND THE MARSHALLVILLE FIRE CONTRACT FOR 2008**

RESOLUTION TO EXTEND THE MARSHALLVILLE FIRE CONTRACT FOR 2008 FOR TWO MONTHS AT A COST OF \$1,666.67 FOR NOVEMBER AND DECEMBER, MOTION BY LENNY BROOME, SECONDED BY JEFF PREBISH, ROLL CALL: ALL AYES.

**08-0147-10 CONTRACT WITH RITTMAN FOR DISPATCHING FOR 2009**

RESOLUTION TO AGREE TO A CONTRACT WITH RITTMAN FOR DISPATCHING FOR 2009, COST \$5,800.00. **NO ACTION AT THIS TIME.**

**08-0148-10 SEND THE EMTS TO THE PEDIATRIC EDUCATION FOR PRE-HOSPITAL PROFESSIONS.**

RESOLUTION TO SEND THE EMTS TO THE PEDIATRIC EDUCATION FOR PRE-HOSPITAL PROFESSIONS AT A COST OF \$145. PER PERSON, THIS WILL BE IN HOUSE. MOTION BY LENNY BROOME, SECONDED BY JEFF PREBISH, ROLL CALL, ALL AYES.

**08-0149-10 PURCHASE FLASH LIGHTS & OTHER EQUIPMENT**

RESOLUTION TO PURCHASE FLASH LIGHTS AND OTHER EQUIPMENT, WHICH INCLUDES GLOVES AND HOODS (THESE WILL BE SPARES), FROM PHOENIX FIRE FOR A COST OF \$500.00. MOTION BY LENNY BROOME, SECONDED BY JEFF PREBISH, ROLL CALL, ALL AYES.

**08-0150-10 PURCHASE MORE UNIFORMS FROM D & G**

RESOLUTION TO PURCHASE MORE UNIFORMS FROM D & G AT A COST OF \$1,000.00. MOTION BY JEFF PREBISH, SECONDED BY LENNY BROOME, ROLL CALL, ALL AYES.

**08-0151-10 ENTER AGREEMENT WITH THE VILLAGE TO INSTALL FIRE HYDRANTS**

RESOLUTION TO RESCIND RESOLUTION 08-0035-03 A RESOLUTION TO ENTER AGREEMENT WITH THE VILLAGE OF DOYLESTOWN TO INSTALL FIRE HYDRANTS. MOTION BY JEFF PREBISH, SECONDED BY LENNY BROOME, ROLL CALL, ALL AYES.

**08-0152-10 ENTER IN A CONTRACT WITH THE VILLAGE OF DOYLESTOWN**

RESOLUTION TO ENTER IN A CONTRACT WITH THE VILLAGE OF DOYLESTOWN TO INSTALL FIRE HYDRANTS. MOTION BY JEFF PREBISH, SECONDED BY LENNY BROOME, ROLL CALL, ALL AYES.

**08-0153-10 APPROVE SUPPLEMENTAL APPROPRIATIONS**

RESOLUTION APPROVING SUPPLEMENTAL APPROPRIATIONS AS FOLLOWS FROM 1000-930-930 TO 1000-420-370 THE AMOUNT OF \$16,000.00 TO MEET CURRENT EXPENSES. MOTION BY LENNY BROOME SECONDED BY JEFF PREBISH, ROLL CALL, ALL AYES.

**08-0154-10 ADVISORY SPEED STUDY BY WAYNE COUNTY ENGINEERS**

RESOLUTION TO HAVE AN ADVISORY SPEED STUDY DONE ON MOINE ROAD BETWEEN 585 AND DOYLESTOWN ROAD. MOTION BY LENNY BROOME, SECONDED BY JEFF PREBISH, ROLL CALL: ALL AYES.

CHIPPEWA TOWNSHIP TRUSTEES SPECIAL

TOWNSHIP HALL

7:00 PM

OCTOBER 27,

08

**AL SCHRADER GAVE US UPDATES ON THE CEMETERY MAPLE GROVE AND PAVKOV PROPERTY.**

**PUBLIC COMMENT: NO COMMENT**

**MOTION TO ADJOURN**

MOTION TO ADJOURN BY LENNY BROOME, SECONDED BY JEFF PREBISH, ROLL CALL, ALL AYES.

MEETING ADJOURNED AT 7:50 PM.

TRUSTEES \_\_\_\_\_

\_\_\_\_\_  
FISCAL OFFICER

\_\_\_\_\_

\_\_\_\_\_