Minutes

Village Board of Trustees

September 12, 2013

A regular meeting of the Village of Horseheads Board of Trustees was held on the above date at 7:00 p.m. Present were:

Village Board and Staff

Mayor Donald Zeigler
Trustee Ron Swartz
Trustee Larry Clark
Trustee George Koliwasky
Trustee Mike Skroskznik
Village Manager Walt Herbst
Clerk-Treasurer Sharron Cunningham
Police Chief Mike Barton

Others Present

Dave Padgett, W. Franklin St.
Joe Ruhmel, Gardner Rd.
Wayne Brubaker, Gardner Road
Glenn, Susan Hostetler, W. Broad St.
Joshua Baker, Steuben St.
Dave, Lois Murray, Lee Ave.
Mary Mower, Kinley Pl.
Jean Quinn, Gardner Rd.
Barb Skorczewski, W. Franklin St.
Brad, Debi Lytle, Grand Central Ave.
Debbie Hicks, Gardner Rd.
Eileen Patocka, Watkins Rd.
Jodi Skroskznik, Center St.
Rob, Kelly Maloney, Westlake St.
Mike Swasta, Watkins Rd.
Susan Multer, Watkins Rd.
Ken Howland, Briarcliff Dr.
Scott McGrain, Gardner Rd.
Brad Layton, W. Franklin St.
News Media

Resolution by Trustee Clark, seconded by Trustee Koliwasky

BE IT RESOLVED, that the reading of the minutes of the Board of Trustees Meetings of August 15, August 29, and September 5, 2013 be dispensed with and the same stand approved as entered by the Clerk.

Roll Call Vote:

Mayor Zeigler	Aye
Trustee Swartz	Aye
Trustee Koliwasky	Aye
Trustee Skroskznik	Aye

Trustee Skroskznik stated he is protesting the minutes of September 5 since he was not in attendance.

Audience Participation

Pat Gross, W. Broad St. – Board should reconsider having its second meeting in the morning. Should also reconsider the firearms policy. They should be off Village property.

Susan Multer, Watkins Rd. – There is an inconsistency on why you changed your meeting times. One Trustee cannot attend the morning meeting. Also, regarding the NYCOM conference, Village cannot afford to spend money we don't have.

Mike Swasta, Watkins Rd. – public hearing should be held so the public can voice their concerns. Also, regarding the connector road, the county is looking for funding for this – they should bond it.

Jodi Skroskznik, Center St. - Village is sad that you represent us. We want answers as to why the meetings changed.

Brad Layton, Grand Central Ave. – Village should do what they did with comprehensive plan. Send a survey to all residents and have them list 12 things they absolutely can't do without.

Scott McGrain, Gardner Rd. – I encourage you to allow the SRO program to continue.

End of audience participation.

Resolution by Trustee Swartz, seconded by Trustee Skroskznik

BE IT RESOLVED, that the audit of bills as listed below be received and approved for payment when in funds:

General:	$	219,801.35
Water:	$	25,023.15
T/A:	$	1,027.44

BE IT FURTHER RESOLVED, that $3,373.00 be transferred from the Capital Reserve Fund for equipment for the new police vehicle.

Roll Call Vote:

Mayor Zeigler	Aye
Trustee Swartz	Aye
Trustee Koliwasky	Aye
Trustee Clark	Aye
Trustee Skroskznik	Aye

Financial Report

Village Manager Herbst – in the general fund revenues are up. We are one of just a handful of Villages that have zero debt. Because of our excellent financial condition our interest rate for the recent bond was 0.83%. This is due to the good work of our staff.

Manager Herbst discussed the requirement by the State for five year planning. There are several issues the Village is now facing – reduction in sales tax, increase in health insurance costs, collective bargaining negotiations, and utility costs.

Resolution by Trustee Koliwasky, seconded by Trustee Swartz

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 require municipal utilities and other departments to implement an identity theft program and policy, and

WHEREAS, The Village of Horseheads Board of Trustees has determined that the attached policy is in the best interest of the municipality and its citizens.

NOW THEREFORE BE IT RESOLVED by the Village of Horseheads Board of Trustees that the attached Identity Theft Policy is hereby approved, a copy of same shall be placed on file in the Village Clerk's Office, and made a part of these minutes.

Roll Call Vote:

Mayor Zeigler	Aye
Trustee Swartz	Aye
Trustee Koliwasky	Aye
Trustee Clark	Aye
Trustee Skroskznik	Aye

Resolution by Trustee Swartz, seconded by Trustee Koliwasky

BE IT RESOLVED, that this Board hereby approves the one year probationary appointment of Nathan P. Stranges, 202 Winding Way, to the Village of Horseheads Fire Department.

Roll Call Vote:

Mayor Zeigler	Aye
Trustee Swartz	Aye
Trustee Koliwasky	Aye
Trustee Clark	Aye
Trustee Skroskznik	Aye

Trustee Skroskznik questioned the waiver of training expenses for former Officer Goodwin. He said the Manager sent a letter to John Burin waiving the reimbursement of fees. This should have gone before the Village Board.

Manager Herbst stated that he felt it was a Managers decision, not a Board's. The entire amount was only $86.66. He added that Officer Goodwin interviewed with Elmira Heights and the City of Elmira before I knew he was leaving.

Trustee Clark – Attended NYCOM conference. Did four classes a day covering many issues.

Trustee Koliwasky – We should have a workshop to discuss the materials received at the NYCOM conference. After brief discussion the Board agreed to the workshop being held on Monday September 23rd at 2pm, noting that there is already a workshop for the same day at 3pm regarding Parks & Recreation.

Mayo Zeigler stated that if anyone has questions they can schedule an appointment with the Village Manager.

As there was nothing further to come before the Board, the meeting was adjourned at 7:45 p.m.

/rmb

IDENTITY THEFT POLICY
Adopted 9/12/13

SECTION 1: BACKGROUND

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

SECTION 2: PURPOSE

The municipality adopts this sensitive information policy to help protect employees, customers, contractors and the municipality 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 municipality in compliance with state and federal law regarding identity theft protection.

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

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 municipality, 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, flex spending plan, health savings account of like plan, check

requests and associated paperwork

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

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personal 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: Municipal 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 NYS Freedom of Information Law and the municipality'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 municipality cannot resolve a conflict between this policy and the NYS Freedom of Information Law, the municipality will contact the Committee on Open Government.

4.A.2: Hard Copy Distribution

Each employee and contractor performing work for the municipality 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 shredding device. Locked shred bins are labeled "*Confidential paper shredding and recycling.*" Municipal records, however, may only be destroyed in accordance with the Village's records retention policy.

4.A.3: Electronic Distribution

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

1. Internally, sensitive information may be transmitted using approved municipal 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 for 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 municipality 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 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 of activity 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.

5.B.3: In order to detect any of the red flags identified above or below upon or prior to the opening of a new account municipal personnel should take one or more of the following steps to obtain and verify the identity of the person opening the account:

1. Requiring identifying information such as name, date of birth, residence or billing address, principal place of business, social security number, drivers license number, or other identification;

2. Verify the customer's identity such as by reviewing a drivers license;

3. Reviewing documentation showing the existence of a business entity, and

4. Independently contacting the customer.

5.B.4: In order to detect any of the red flags identified above or below for an existing account, municipal personnel should take one or more of the following steps to monitor transactions with an account:

1. Verifying the identify of customers if they request information.

2. Verify the validity of requests for change in billing addresses; and

3. Verify changes in banking information.

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 the municipality, 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 municipality. 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
- 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.

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

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

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 municipality 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).

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 municipality is notified that the customer is not receiving paper account statements.

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

5.E.8: The municipality receives 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 municipality

5.E.9: The municipality 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 municipality from damages and loss.

6.A.1: Once potentially fraudulent activity is detected, gather all related documentation and write a summary of the situation. Present this information to the Program Administrator for determination.

6.A.2: The Program Administrator will oversee 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 appropriate law enforcement;
3. Determining the extent of liability of the municipality; and
4. Notifying the actual customer that fraud has been attempted.

SECTION 7: PERIODIC UPDATES TO PLAN

At least annually the Program Administrator will consider the municipality's experiences with identify theft situations, changes in identify theft methods, changes in identity theft detection and prevention methods, changes in the municipality's business arrangements with other entities, etc. After considering these factors, the Program Administrator will determine whether changes to the program, including the listing of red flags, are warranted. If warranted the Program Administrator will present the Village Board with recommended changes, and the Village Board will make a determination of whether to accept, modify or reject the recommendations.

SECTION 8: PROGRAM ADMINISTRATION

8.A: Oversight

The municipality's program will be overseen by a Program Administrator. The Program Administrator shall be the Village Manager. The Program Administrator will be responsible for the program's administration, for insuring appropriate training of municipal staff, for reviewing staff reports for detection of red flags and the steps for preventing and mitigating identity theft, determining which steps of prevention and mitigation should be taken in particular circumstances, reviewing and if necessary approving changes to the program. The Program Administrator shall have the authority to delegate any or all of such oversight responsibilities.

8.B: Staff training and reports

Municipal staff responsible for implementing and overseeing the program shall be trained either by or under the direction of the Program Administrator in the detection of Red flags and the

responsive steps to be taken when a red flag is detected. Such staff may be required to provide reports to the Program Administrator on incidents of identity theft, the municipality's compliance with the program and the effectiveness of the program.

8.C: Service provider arrangements

In the event that the municipality engages a service provider to perform an activity in connection with one or more accounts, the municipality will take the following steps to insure that the service provider performs its activities in accordance with reasonable policies and procedures designed to detect, prevent and mitigate the risk of identity theft. These steps may include 1) requiring by contract that service providers have such policies and procedures in place; 2) requiring by contract that the service providers review the municipality's program and report any red flags to the Program Administrator. 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 meet the requirements of the municipality's program.

/rmb