EXHIBIT 1

The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned after its submission. By providing this notice, the Town of Winthrop, Maine does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Nature of the Data Event

On September 14, 2022, Winthrop Police Department ("Winthrop PD") became aware of a social engineering scheme that resulted in the transfer of certain police department records from a Winthrop PD employee to an unauthorized individual via email. The transfer occurred in response to a phishing email, which was sent by the unauthorized individual to the Winthrop PD employee and purported to be from an employee of a state agency with whom the Winthrop PD employee works regularly. Believing the email to be legitimate, the Winthrop PD employee sent the requested information in response, which included certain Maine residents' personal information.

The information made accessible to an unauthorized individual and potentially viewed or acquired includes name and Social Security number.

Notice to Maine Residents

On October 5, 2022, Winthrop PD provided written notice of this incident to three (3) Maine residents. Written notice was provided in substantially the same form as the letter included herewith as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering this incident, Winthrop PD moved quickly to investigate and respond, assess the security its systems, and identify potentially affected individuals. Further, Winthrop PD is taking steps to enhance email security, including by increasing protections to its firewall, enhancing email filtering mechanisms, and broadening workforce training on the topics of data privacy and detection of social engineering schemes.

As an added precaution, Winthrop PD is providing potentially affected individuals with access to complimentary credit monitoring and identity restoration services for one year through TransUnion.

Additionally, Winthrop PD is providing potentially affected individuals with guidance on how to protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Winthrop PD is also providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

EXHIBIT A

Winthrop Police Department

15 Town Hall Lane
Winthrop, Maine 04364
Phone: 207-377-7226
Fax: 207-377-7229
wpdadmin@winthropmaine.org

Chief Ryan M. Frost
Lieutenant Peter Struck

[First Name] [Last Name]
[Address 1]
[Address 2]
[City], [State] [Zip]

October 5, 2022

Notice of Security Incident

Dear <<Name 1>> <<Name 2>>:

The Winthrop Police Department ("We" or "Winthrop PD") is writing to inform you of an email phishing event that may impact the privacy of some of your information. We are providing you with details about the event, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so. We value and respect the privacy of those we serve.

What Happened? On September 14, 2022, we became aware of a social engineering scheme that resulted in the transfer of certain police department records from a Winthrop PD employee to an unauthorized individual via email. The transfer occurred in response to a phishing email, which was sent by the unauthorized individual to the Winthrop PD employee and purported to be from an employee of a state agency with whom the Winthrop PD employee works regularly. Believing the email to be legitimate, the Winthrop PD employee sent the requested information in response, which included your name and Social Security number. Upon learning of this event, we worked quickly and diligently to confirm what occurred and provide this notice to individuals whose information might be affected as a result.

What Information Was Involved? We cannot confirm if the unauthorized person(s) accessed or viewed any specific information relating to you. However, as indicated above, we determined that the information transferred and therefore accessible included your name and Social Security number.

What We Are Doing. We are committed to protecting the confidentiality, privacy, and security of the information we collect in providing services to town residents and others. As such, we are taking steps to enhance email security, including by increasing protections to our firewall, enhancing email filtering mechanisms, and broadening workforce training on the topics of data privacy and detection of social engineering schemes.

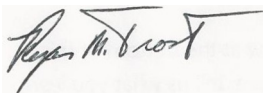
As an added precaution, we are also providing you with access to 12 months of complimentary credit monitoring and identity restoration services through TransUnion, along with guidance on how to better protect against the possibility of information misuse. We are covering the cost of these services, but due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions included within the enclosure to this letter.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanations of benefits, as applicable, and by monitoring your free credit reports for suspicious activity. You can find out more about how to better protect against the potential misuse of information in the enclosed *Steps You Can Take to Protect Information.* There, you will also find more information about the credit monitoring services we are offering and how to enroll.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call us at (207) 377 - 7225, 8:30am – 4:30pm excluding U.S. holidays.

We apologize for any inconvenience this event may cause you and remain committed to the privacy of information in our possession.

Sincerely,



Chief Ryan M. Frost

Steps You Can Take to Protect Information

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code," enter the following unique 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **697871** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and **January 31, 2023.** Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am-9pm, Saturday-Sunday: 8am-5pm Eastern time.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.