



Joshua P. Brian
 T: (850) 205-3336 F: (850) 681-9792
 joshua.brian@nelsonmullins.com

NELSON MULLINS RILEY & SCARBOROUGH LLP
 ATTORNEYS AND COUNSELORS AT LAW

215 South Monroe Street, Suite 400
 Tallahassee, FL 32301
 T: 850.681.6810 F: 850.681.9792
 nelsonmullins.com

RECEIVED
 MAR 20 2020
 CONSUMER PROTECTION DIV

March 17, 2020

Via Certified Mail and E-mail To: attorney.general@doj.nh.gov

Attorney General Gordon J. MacDonald
 33 Capitol Street
 Concord, NH 03301

RE: Town of Houlton Police Department Notice of Data Security Incident

Dear Attorney General MacDonald:

Our law firm, Nelson Mullins Riley & Scarborough LLP, 215 South Monroe Street, Ste. 400, Tallahassee, FL 32301, represents the Town of Houlton Police Department (“Police Department”), 97 Military Street, Houlton, ME 04730, a municipal law enforcement agency. The Police Department experienced a ransomware attack and will be sending the one (1) potentially affected New Hampshire resident the enclosed written notice with an offer of twelve (12) months of Kroll identity monitoring without cost.

The circumstances of the data security incident are that on October 16, 2019, Police Department personnel became aware that files within a portion of its network were inaccessible, which was subsequently determined to be from a ransomware attack. The Police Department restored its data from maintained backups.

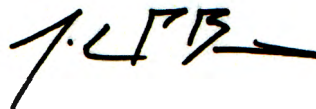
As a result of this incident, the Police Department engaged an industry-leading forensic investigation firm and tasked them to determine the scope of the compromise and identify any data accessed or acquired collateral to the ransomware event. After a thorough analysis of all available forensic evidence, the firm determined the Police Department information technology environment was compromised by malware from October 15, 2019, to October 16, 2019, and that an unauthorized individual or individuals gained access to part of the network between January 25, 2019, and October 15, 2019. The firm, however, was unable to determine what specific information was accessed or acquired or whether a breach occurred via access to or acquisition of data containing New Hampshire residents’ information. In an abundance of caution, the Police Department engaged a data mining vendor to review all potentially accessed data for personal information which, after addition and updating of contact information, was completed on February 26, 2020. The data mining revealed personal information for one (1) New Hampshire resident was contained in the reviewed data.

With respect to the one (1) New Hampshire resident, the personal information consisted of a first and last name and financial account number *without* any security code, access code, or password to access the account. The New Hampshire resident will be notified by the enclosed letter post-marked March 17, 2020.

March 17, 2020
Page 2

Please let me know if you have any additional questions regarding this notification.

Very truly yours,

A handwritten signature in black ink, appearing to read 'J. P. Brian', with a horizontal line extending to the right.

Joshua P. Brian

Enclosure: Notice to New Hampshire Resident



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

The Town of Houlton Police Department respects the privacy of your information, which is why we are writing to tell you about a data security incident that may have exposed some of your personal information. We take the safeguarding and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the data security incident.

What Happened

On October 16, 2019, we learned that part of our network was infected with a virus that prohibited access to our files. We quickly restored our systems from backups and then engaged an industry-leading forensic investigation firm to determine the nature and scope of this incident. After a thorough analysis of all available forensic evidence, the investigation determined the encryption malware was active on our network from October 15, 2019 to October 16, 2019. We determined that the virus was introduced by an unknown individual or individuals outside our organization who gained access to part of our network between January 25, 2019 and October 15, 2019. The forensic investigation firm was unable to determine, however, what information, if any, was accessed or acquired by the unauthorized individual or individuals responsible for encrypting our files.

Due to the forensic investigation firm's findings, we requested an additional firm review all available data in the accessed portion of the network to determine whether it included personal information. The review, after addition of contact information, was completed on February 26, 2020, and revealed that some of the folder directories contained personal information for certain individuals, including you.

The forensic investigation could not conclude that any of your personal information was accessed or acquired by an unauthorized individual. However, in an abundance of caution, we are providing you with notice of the possible unauthorized disclosure and one (1) year of identity monitoring at no cost to you to allow you to take steps to help protect your personal information, if you feel it is appropriate to do so.

What Information Was Involved

We are unable to confirm whether your information was actually accessed or obtained by an unauthorized individual. Our investigation determined that, as a result of this incident, some of your personal information may conceivably have been accessed and acquired without authorization, including your <<b2b_text_1(Impacted Data)>>.

We are notifying you so you can take appropriate steps to help protect your personal information.

What We Are Doing

To help relieve concerns following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one (1) year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **June 26, 2020** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter. We encourage you to review the description and to consider activating the offered services.

Rest assured that we are committed to keeping the data we maintain as secure as possible. We are taking steps to minimize the potential for unauthorized access to our environment and making reasonable efforts to ensure the continued security of your information.

What You Can Do

Please review the enclosed "Additional Resources" information included with this letter, which describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

For further information, please call 1-877-594-0964, Monday through Friday, from 9:00 a.m. to 6:30 p.m. Eastern Time. We take the safeguarding of your personal information very seriously and apologize for any inconvenience this incident may cause you. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Timothy B. DeLuca

Chief Timothy B. DeLuca
Houlton Police Department

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, P.O. Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, P.O. Box 34012, Fullerton, CA 92834, www.transunion.com, 1-800-916-8800

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity over the next twenty-four months, and immediately report incidents of suspected identity theft to both your financial provider and law enforcement.

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. You may also seek to have information relating to fraudulent transactions removed from your credit report. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report free of charge.

A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) legible copy of a government issued identification card; (6) legible copy of a recent utility bill or bank or insurance statement that displays your name and current mailing address, and the date of issue; and (7) any applicable incident report or complaint filed with a law enforcement agency.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, <https://www.consumer.ftc.gov/features/feature-0014-identity-theft>, 1-877-IDTHEFT (438-4338).

State Attorney General's Office Contact Information. <<b2b_text_2(State AG Office Info)>>.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.