



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

RECEIVED

AUG 16 2021

CONSUMER PROTECTION

Samuel Sica, III  
Office: (267) 930-4802  
Fax: (267) 930-4771  
Email: [ssica@mullen.law](mailto:ssica@mullen.law)

426 W. Lancaster Avenue, Suite 200  
Devon, PA 19333

August 12, 2021

**VIA U.S. MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent the Borough of Haledon Police Department (“Haledon”) located at 510 Belmont Avenue, Haledon, NJ 07508, and are writing to notify your office of an incident that may affect the security of some personal information relating to approximately thirteen (13) New Hampshire residents. This notice may be supplemented if new significant facts are learned subsequent to its submission. By providing this notice, Haledon does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

On July 10, 2020, Haledon became aware of suspicious activity relating to its systems and immediately launched an investigation, along with third-party computer forensic specialists, to determine the nature and scope of the activity. Haledon also reported the activity to the Federal Bureau of Investigation and assisted with its investigation. Haledon determined that an unknown actor gained access to certain Haledon systems on or about June 2, 2020. The unknown actor claimed to have removed certain databases from the Haledon network.

Although the investigation was unable to confirm which specific files, if any, were impacted, Haledon could not rule out the possibility that individuals’ information may have been impacted. Therefore, in an abundance of caution because of the uncertainty of the event, Haledon undertook a comprehensive and time-intensive review of all files that could have been impacted. This review was recently completed and determined that information relating to individuals was present in potentially impacted databases.

The information for New Hampshire residents contained in the potentially impacted databases includes name, Social Security number, and driver’s license number.

**Mullen.law**

### **Notice to New Hampshire Residents**

On August 12, 2021, Haledon began mailing notice of this incident to potentially affected individuals, which includes approximately thirteen (13) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, Haledon moved quickly to investigate and respond to the incident, assess the security of Haledon's systems, and notify potentially affected individuals. Haledon is also working to implement additional safeguards. Haledon is providing access to credit monitoring and identity restoration services for one (1) year, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Haledon is also providing contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident.

Additionally, Haledon is providing impacted individuals with guidance on how to better 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. Haledon is 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. Haledon also reported this incident to federal law enforcement and other state regulators.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4802.

Very truly yours,



Samuel Sica, III of  
MULLEN COUGHLIN LLC

SZS/zlg  
Enclosure

# EXHIBIT A



Return Mail Processing Center  
P.O. Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<Address 4>>  
<<Address 5>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

<<Variable Header>>

Dear <<Name 1>>:

The Borough of Haledon Police Department (“Haledon”) is writing to notify you of a recent event that may involve some of your information. Although at this time there is no indication that your information has been fraudulently misused in relation to this incident, we are providing you with information about the incident, our response to it, and additional measures you can take to protect your information, should you feel it appropriate to do so.

**What Happened?** On July 10, 2020, Haledon became aware of suspicious activity relating to its systems and immediately launched an investigation to determine the nature and scope of the activity. Haledon determined that an unknown actor gained access to certain Haledon systems on or about June 2, 2020. The unknown actor claimed to have removed certain databases from our network.

Although the investigation was unable to confirm which specific files, if any, were impacted, we could not rule out the possibility that some of your information may have been impacted. Therefore, in an abundance of caution because of the uncertainty of this event, Haledon undertook a comprehensive and time-intensive review of all files that could have been impacted. This review was recently completed and determined that your information was present in potentially impacted databases.

**What Information Was Involved?** Our investigation determined that at the time of the incident, your name and <<Breached Elements>> were stored within potentially impacted databases. To date, Haledon has not received any reports of fraudulent misuse of any information potentially impacted by this event.

**What We Are Doing.** The confidentiality, privacy, and security of your information are among our highest priorities, and we have security measures in place to protect information in our systems. Upon learning of the activity, we immediately took steps to secure our systems and investigate the event. Haledon’s vendors deployed advanced endpoint monitoring tools to the network and secured access credentials in response to the event. We notified the Federal Bureau of Investigation of the event and assisted in its investigation. We are also notifying certain state regulators, as necessary.

While we are unaware of any fraudulent misuse of your information as a result of this incident, as an additional precaution, Haledon is offering you access to twelve (12) months of complimentary credit monitoring services through TransUnion. Details of this offer and instructions on how to activate these services are enclosed with 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 monitoring your free credit reports for suspicious activity and to detect errors. Please also review the enclosed document, “Steps You Can Take to Help Protect Your Information,” which contains information on what you can do to safeguard against possible misuse of your information. You can also enroll in the credit monitoring services that Haledon is offering to you.

***For More Information.*** If you have additional questions or concerns, please contact our toll-free dedicated assistance line at 866-991-0883. This toll-free line is available Monday – Friday from 9 am to 9 pm Eastern Time (excluding U.S. holidays). You may also write to Haledon at 510 Belmont Avenue, Haledon, NJ 07508.

We apologize for any inconvenience or concern this incident may cause.

Sincerely,

***Chief Angelo J. Daniele***

Angelo J. Daniele  
Chief of Police  
Borough of Haledon Police Department

## Steps You Can Take to Help Protect Your Information

### **Enroll in Complimentary Credit Monitoring**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion,<sup>®</sup> one of the three nationwide credit reporting companies.

### **How to Enroll: You can sign up online or via U.S. mail delivery.**

- To enroll in this service, go to the *myTrueIdentity* website at [www.MyTrueIdentity.com](http://www.MyTrueIdentity.com) and, in the space referenced as "Enter Activation Code," enter the 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 six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> 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.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. 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 a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

### **ADDITIONAL DETAILS REGARDING YOUR 12-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score.
- 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, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

### **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](http://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
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
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](http://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.

*For District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 441 4th St. NW #1100 Washington, D.C. 20001; 202-727-3400; and [oag@dc.gov](mailto:oag@dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us).

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are **XX** Rhode Island residents impacted by this incident.

*For New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.