MELANIE MARIE WITTE
415.477.5731 telephone
melanie.witte@troutmansanders.com

TROUTMAN SANDERS

TROUTMAN SANDERS LLP
Attorneys at Law
580 California Street, Suite 1100
San Francisco, CA 94104
415.477.5700 telephone
troutmansanders.com

June 2, 2017

OVERNIGHT

Attorney General Joseph Foster
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Incident

Dear Attorney General Foster:

Pursuant to N.H. Rev. Stat. Ann. section 359-C:20, and on behalf of my client the Township of Springfield, I am writing to notify you of a data incident potentially affecting two (2) New Hampshire residents.

NATURE OF THE UNAUTHORIZED ACCESS

During a network security review, the Township of Springfield identified suspicious activity on their Police Department management server. Once they discovered this suspicious activity, they immediately initiated an internal investigation and IT remediation. The Township also engaged external forensic IT experts to assist in their investigation, and the incident was subject to ongoing police investigation. The forensic IT experts have confirmed that there was unauthorized access to the server through brute force between Feb. 22, 2017 and March 9, 2017, when the threat was eliminated.

The information may have included New Hampshire residents': full name, driver's license or state card identification number, birth date, address, and telephone number.

NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED

Two (2) New Hampshire residents were potentially affected as a result of the unauthorized access. The residents will be mailed a notification letter on Tuesday, June 6, 2017. Please see enclosed for a form version of the notice.

STEPS WE HAVE TAKEN RELATING TO THE INCIDENT

In addition to the steps immediately taken in response to this event, the Township of Springfield remains vigilant in its efforts to protect confidential information of its citizens and visitors and has already implemented additional safeguards to help prevent additional cyber-attacks. They also continue to work closely with the FBI, and they have been in continual communication with the New Jersey State Police, all applicable state agencies, and all three credit bureaus. Lastly, the Township will pursue prosecution of these criminals to the full extent of U.S. law.

Credit Monitoring and Identity Repair Services are being provided for two years through AllClear ID when either a driver's license or state card identification number is potentially involved (though again, there is no evidence that any personal information has been viewed or used inappropriately). Further, a dedicated call center will be available.

OTHER NOTIFICATION AND CONTACT INFORMATION

Formal notification letters to all potentially impacted individuals are being mailed Tuesday, June 6, 2017, the applicable state Attorney General offices and consumer affairs agencies have been notified, and the Township of Springfield is continuing to actively work with the FBI in their ongoing investigation.

For any further information, please contact Melanie Witte at (415) 477-5731, melanie.witte@troutmansanders.com, Troutman Sanders, 580 California Street, Suite 1100, San Francisco, CA 94104.

Sincerely,

Melanie Marie Witte

Enclosure

Processing Center • P.O. BOX 141578 • Austin, TX 78714

00031
ACD1234

21631
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

June 6, 2017

NOTICE OF DATA BREACH

Dear John Q. Sample:

The Township of Springfield ("Township") values and respects your privacy; accordingly, we are writing to advise you about an incident involving potential exposure of some of your personal information. Below, we've outlined steps the Township has undertaken since discovering the incident, and provided guidance on general best practices for identity theft protection.

It is important to note that, at this time, we have no indication that any personal information has been viewed or used inappropriately. However, out of an abundance of caution, we are providing notice to individuals identified as potentially affected.

What Happened?

As a result of a network security review, we identified suspicious activity on our Police Department management server. Once we discovered this suspicious activity, we immediately initiated an internal investigation and IT remediation. We also engaged external forensic IT experts to assist in our investigation, and the incident was subject to ongoing police investigation. The forensic IT experts have confirmed that there was unauthorized access to the server between Feb. 22, 2017 and March 9, 2017, when the threat was eliminated.

What Information Was Involved?

The information may have included your full name, driver's license or state card identification number, birth date, address, and telephone number. Each individual may have been impacted differently. For additional information on what information might have been impacted, please call toll free number 1-855-361-3678.

What We Are Doing.

In addition to the steps immediately taken in response to this event, the Township remains vigilant in its efforts to protect confidential information of its citizens and visitors and has already implemented additional safeguards to help prevent additional cyber-attacks. We also continue to work closely with the FBI, and we have notified the New Jersey State Police, all applicable state agencies, and all three credit bureaus. Lastly, we will pursue prosecution of these criminals to the full extent of U.S. law.

While we have no indication that any personal information has been accessed or used inappropriately, as an added precaution, the Township is also providing you with 24 months of complimentary identity repair and credit monitoring. Both services start on the date of this notice, and you can use them at any time during the next 24 months. However, AllClear Credit Monitoring, which includes a $1 million identity theft insurance policy, requires you to sign up.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-361-3678 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service has also been prepaid for you for 24 months, but it requires you to enroll. It offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. Details of the insurance policy can be found at https://www.allclearid.com/insurance. To enroll, you may sign up online at enroll.allclearid.com or by phone by calling 1-855-361-3678 using the following redemption code: Redemption Code.*

*Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

What You Can Do.

In addition to signing-up for the complimentary credit monitoring we have secured for you, we encourage you to review the enclosed "Information about Identity Theft Protection" for best practices on protecting your information.

For More Information.

If you have questions or need additional information, please call toll free number 1-855-361-3678, Monday through Saturday, from 9 A.M. to 9 P.M. EST. You may also call (973) 912-2285, or write us at 100 Mountain Avenue, Springfield, NJ 07081.

We regret any concern or inconvenience this matter may have caused you and appreciate your patience and understanding.

Sincerely,

Diane Stampoulos
Mayor
Township of Springfield

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax:	P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian:	P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion:	P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

For residents of Rhode Island: You may contact the Attorney General's Office at http://www.riag.ri.gov/ or (401) 274-4400

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008, www.equifax.com
Experian:	1-888-397-3742, www.experian.com
TransUnion:	1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at*

each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax:	P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian:	P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC:	P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077