100 E Main St.
Christiansburg, VA 24073

November 26, 2018

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

RE: Security Breach Notification

To Whom It May Concern:

I serve as the Town Manager of the Town of Christiansburg, and provide this notification to you of a recent data security incident suffered by the Town. On October 26, 2018, computer forensics revealed that three Town of Christiansburg employee accounts were compromised following a phishing email attack from May 17th, June 6th and September 2018. Upon learning that the accounts were compromised, the log in information for all employee accounts was changed and has been constantly monitored by computer forensics. We also contacted local law enforcement. As a result of these incidents, personal information of 909 individuals, including 1 New Hampshire resident, was subjected to unauthorized access. This includes some combination of an individual's social security number, financial account information, driver's license numbers, credit card information, username and password combinations and passport information.

We promptly notified the affected individuals on November 26, 2018 and have provided them with complimentary credit monitoring. A copy of the formatted letter is attached. As the letter indicates, the Town will be offering credit monitoring and identity restoration services for one year at the Town's expense. We are taking steps to comply with all applicable notification obligations.

Please contact me should you have any questions.

Sincerely,

Randy Wingfield
Town Manager

Return Address

November 26, 2018

Sample
[redacted]

RE: Important Security Notification. Please read this entire letter.

Dear Sir or Madam:

We are contacting you regarding a data security incident. On October 26, 2018, computer forensics revealed that three Town of Christiansburg employee accounts were compromised following a phishing email attack from May 17th, June 6th and September 2018. Upon learning that the accounts were compromised, the log in information for all employee accounts was changed and has been constantly monitored by computer forensics. We also contacted local law enforcement. As a result of these incidents, personal information of 909 individuals was subjected to unauthorized access. This includes some combination of your social security number, financial account information, driver's license numbers, credit card information, username and password combinations and passport information. As a result, your personal information may have been exposed to others.

What Did We Do to Protect Your Information?

Please be assured that the Town of Christiansburg has taken every step necessary to address the incident, and that we are committed to fully protecting all of the information that you have entrusted to us. The Town of Christiansburg worked with data privacy experts and other professionals to further protect your privacy. We are concerned about both our valued customers and work force. We have already taken steps to fix the issue and strengthen our systems, and will continue to do so throughout this response process and beyond. We have also implemented the following protective measures:

- Requiring security and data protection training for all employees;
- Implementing additional technological security measures;
- Updating our password protocols;
- Limiting user's access to information possessed and maintained by Town of Christiansburg; and
- Conducting regular phishing testing of our employee and network.

In addition, and to help protect your identity, we are offering a complimentary one-year membership in Experian's Credit 1-Bureau.This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with

an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks ^{SM} as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- **Ensure that you enroll by February 28, 2019** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **www.experianidworks.com/credit**
- Provide your **activation code**:

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (877) 769-5558 by February 28, 2019. Be prepared to provide engagement number DB09649 as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 12-Month Experian IndentityWorks Membership
A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE^{TM}**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do to Protect Your Information

Please remain vigilant by reviewing account statements and monitoring free credit reports. There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to the enclosed list of additional actions to reduce your chance of identity theft below. Also, please refer to www.ExperianIDWorks.com/restoration for this information. As we go through this process I would ask the following:

1. Please let us know if you learn of or experience any suspicious activity with your credit cards, bank accounts or tax return processing. If you suspect identity fraud, you should report it to a law enforcement agency as you may be able to file a police report. We will cooperate with any investigations that state and federal law enforcement open, and provide any information we can to assist their efforts.

2. Trust that we are doing, and will continue to do, everything possible to protect your personal information and reduce the likelihood of any further problems.

We sincerely apologize for this incident and regret any inconvenience it may cause you. Should you have questions or concerns regarding this matter, please do not hesitate to contact us at (877) 769-5558.

Sincerely,

Randy Wingfield
Town Manager

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90-day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

Equifax
1-800-525-6285
www.equifax.com

Experian
1-888-397-3742
www.experian.com

TransUnion

1-800-680-7289
www.transunion.com

- **PLACE A SECURITY FREEZE ON YOUR CREDIT FILE**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies.

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS**

Visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

- **MANAGE YOUR PERSONAL INFORMATION**

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements.
Be proactive and create alerts on credit cards and bank accounts to notify you of activity.
If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE**

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

  - Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.

  - The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft.

- Individuals can obtain information about steps to avoid identity theft from any of the above credit reporting agencies or the Attorney General.