MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

James Paulino
Office: (267) 930-4741
Fax: (267) 930-4771
Email: jpaulino@mullen.law

75 S. Clinton Avenue, Suite 510
Rochester, NY 14604

April 8, 2022

**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 Allen & Major Associates, Inc. ("Allen & Major") located at 100 Commerce Way, Suite 5, Woburn, Massachusetts 01801, and are writing to notify your office of an incident that may affect the privacy of certain personal information relating to one (1) New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Allen & Major 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 or about February 24, 2022, Allen & Major became aware of unusual activity in its email system. Allen & Major immediately launched an investigation into the incident, with the assistance of third-party computer forensic specialists. That investigation determined that an unauthorized person or persons gained access to certain Allen & Major email accounts between September 2, 2021 and February 24, 2022. As a result, Allen & Major took steps to identify what information was contained within the folders and files of the email accounts involved, and to whom that information related. Allen & Major then took steps to identify contact information for the potentially impacted individuals, which was completed on or about March 10, 2022.

Allen & Major's investigation determined that a single employee mailbox contained information affiliated with the one (1) New Hampshire resident potentially impacted by this incident; however, that information was related to the personal activities of an Allen & Major employee. Allen & Major did not receive the information in the regular course of business and does not believe that it

has notification obligations pursuant to New Hampshire law. Nevertheless, in an abundance of caution, Allen & Major is providing notice and 24 months of credit monitoring to the potentially impacted New Hampshire resident. Moreover, Allen & Major cannot confirm whether any specific information relating to a New Hampshire resident was actually accessed or acquired by an unauthorized individual.

The information that could have been subject to unauthorized access includes name and Social Security number.

**Notice to New Hampshire Residents**

On or about April 8, 2022, Allen & Major provided written notice of this incident to one (1) 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, Allen & Major moved quickly to investigate and respond to the incident, assess the security of Allen & Major systems, and identify potentially affected individuals. Allen & Major is also working to implement enhanced security measures, and is reviewing and enhancing existing policies and procedures. Allen & Major is providing access to credit monitoring services for 24 months, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Allen & Major is providing notice to potentially affected individuals, which includes guidance on how to better protect against identity theft and fraud, including 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. Allen & Major is also providing potentially affected individuals with access to credit monitoring and identity theft restoration services at no cost to these individuals.

Allen & Major also notified the Federal Bureau of Investigation and is also providing written notice of this incident to other relevant state regulators as appropriate.

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4741.

Very truly yours,

James Paulino of
MULLEN COUGHLIN LLC

JMP/dtg
Enclosure

# EXHIBIT A

<<Return Mail Address>>

<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

<<Date>>

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

Allen & Major Associates, Inc. ("Allen & Major") is writing to inform you about an incident that may involve some of your information. Allen & Major takes the protection of personal information very seriously and, although we have no evidence of actual or attempted misuse of your information, this letter provides you with information about the incident, our response, and steps you may take to better protect your information, should you feel it is appropriate to do so. We are also offering you 12 months of complimentary credit monitoring and identity protection services; enrollment instructions can be found in the following pages.

**What Happened?** On or about February 24, 2022, Allen & Major became aware of unusual activity in its email system. Allen & Major immediately launched an investigation into the incident, with the assistance of third-party computer forensic specialists. That investigation determined that an unauthorized person or persons gained access to certain Allen & Major email accounts between September 2, 2021 and February 24, 2022. As a result, we took steps to identify what information was contained within the folders and files of the email accounts involved, and to whom that information related. Allen & Major then took steps to identify contact information for the impacted individuals, including you, which was completed on March 10, 2022.

**What Information Was Involved?** Although we are unaware of any actual or attempted misuse of your information, we are providing this notification out of an abundance of caution because certain information relating to you may have been impacted, including your name and Social Security number. Again, there is no indication that your information has been subject to actual or attempted misuse.

**What We Are Doing**. We take this incident and the security of personal information seriously. Upon discovering this incident, we promptly initiated an investigation and took steps to secure our email system. While we have existing safeguards in place, as part of our ongoing commitment to the privacy of personal information, we are working to implement enhanced security measures, and are reviewing and enhancing existing policies and procedures to reduce the likelihood of a similar future event. As an added precaution, we are providing you with access to complimentary credit monitoring services through Equifax for 24 months. Information on how to enroll in these services is included in the *Steps You Can Take to Help Protect Your Personal Information* section of this letter.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud and to review your account statements and free credit reports for suspicious activity and to detect errors. We also encourage you to review the *Steps You Can Take to Help Protect Your Personal Information* section of this letter.

Sincerely,

Allen & Major Associates, Inc.

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR PERSONAL INFORMATION

### Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service provided by Equifax,® one of the three nationwide credit reporting companies. To enroll in credit monitoring please follow the instructions below.

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of *<ACTIVATION CODE>* then click "Submit" and follow these 4 steps:

1. **Register:** Complete the form with your contact information and click "Continue".
   *If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.*
   *Once you have successfully signed in, you will skip to the Checkout Page in Step 4*
2. **Create Account:** Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:** To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   **You're done!**
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

You can sign up for these services anytime between now and July 31, 2022. You will need to activate these services yourself, as we are not able to do so on your behalf.

### 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 credit 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, etc.); and
7. A copy of either a 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 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 |

**Internal Revenue Service Identity Protection PIN (IP PIN)**

You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

**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.