FMG LAW
Freeman Mathis & Gary LLP

1600 Market Street
Suite 1210
Philadelphia, PA 19103-7240

Tel: 267.758.6009

www.fmglaw.com

Nicholas Jajko
Partner
D: 215.279.8070
nicholas.jajko@fmglaw.com

July 13, 2022

Via Regular U.S. Mail
Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

RE: KMJ Corbin & Company LLP - Notice of Data Breach

Dear Sir or Madam:

We represent KMJ Corbin & Company LLP ("KMJ"), which is a locally owned full-service public accounting firm based in Irvine, California. This submission is provided pursuant to the New Hampshire data breach notification statute, N. H. REV. STAT. §359-C:19, *et seq*. (2007) which requires notice to your office in the event of a breach in the security of personal information affecting residents of the State of New Hampshire.

On October 22, 2021, KMJ discovered suspicious activity involving a KMJ employee's email account. Upon discovery, KMJ commenced an investigation that included working with computer forensics professionals to understand the nature and scope of the incident. Following the conclusion of the investigation, KMJ determined that certain employee email accounts were accessed by an unauthorized person outside the KMJ organization. KMJ cannot confirm with certainty, however, when the access began or which emails, if any, within the affected accounts were specifically accessed by the unauthorized person. KMJ knows that because some emails or documents within the accounts contained individuals' personal information, it is possible the unauthorized person viewed or acquired that information. Therefore, KMJ conducted a review of the entire contents of the accounts beginning on December 13, 2021, and are now notifying potentially affected individuals of this incident out of an abundance of caution. The review concluded on June 10, 2022.

On or about July 13, 2022, KMJ provided notice via U.S. regular mail of the incident to the potentially affected individuals. A sample copy of the notice is attached as Exhibit "A" for your

records. KMJ provided this notification to a total of 1,130 individuals, one (1) of which is a resident of the State of New Hampshire.

As an added precaution, KMJ offered the affected New Hampshire resident twelve (12) months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services (through IDX). The notice to the affected individuals includes instructions on the use of this product as well as encouragement to remain vigilant for incidents of fraud or misuse, by reviewing and monitoring account statements and credit reports, immediately reporting errors or suspicious activity to the financial institution or issuing bank, and filing a report with law enforcement, their state attorney general, and/or the Federal Trade Commission in the event fraud or misuse is discovered. KMJ also included contact information for the major consumer reporting bureaus, state-specific regulators, and additional steps individuals may take to protect the impacted information from misuse, should they find it appropriate to do so.

After discovering the incident, KMJ reset account passwords for all logins to KMJ email accounts in order to enhance the existing protections on its email system. KMJ reported the incident to federal law enforcement. KMJ also partnered with computer forensics professionals to thoroughly investigate, commenced a review of the entire contents of the accounts, notified potentially affected individuals about it, and are now continuing to evaluate ways to strengthen the security of our network going forward. KMJ is also notifying other state regulators as necessary.

I believe this provides you with all information necessary for your purposes and to comply with New Hampshire law. However, if anything further is needed, please contact me directly.

Respectfully,

FREEMAN MATHIS & GARY, LLP

Nicholas Jajko

Exhibit "A"

KMJ Corbin & Company
Business Advisors. Tax and Audit

10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

July 13, 2022

RE: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

We at KMJ Corbin & Company LLP ("KMJ") take the issue of privacy and security of our current and former client information seriously. As part of that commitment, we are writing to inform you of a recent data security incident that may have affected your personal information. Please read this letter carefully.

What Happened?

On October 22, 2021, we discovered suspicious activity involving a KMJ employee's email account. Upon discovery, we commenced an investigation that included working with computer forensics professionals to understand the nature and scope of the incident. Following the conclusion of the investigation, we determined that certain employee email accounts were accessed by an unauthorized person outside the KMJ organization. We cannot confirm with certainty, however, when the access began or which emails, if any, within the affected accounts were specifically accessed by the unauthorized person. We know that because some emails or documents within the accounts contained individuals' personal information, it is possible the unauthorized person viewed or acquired that information. Therefore, we conducted a review of the entire contents of the accounts beginning on December 13, 2021 and are now notifying potentially affected individuals of this incident out of an abundance of caution. The review concluded on June 10, 2022.

What Information Was Involved?

You are receiving this letter because one or more emails and/or attachments containing your personal information, including your <<Variable Data 1>>, could have been accessible and therefore, viewed as a result of the compromise. However, we reiterate that our investigation did not definitively confirm that this occurred, and we have no knowledge of any actual misuse of personal information as a result of this incident at this time. Nonetheless, we believe it is important to notify you about this potential compromise out of an abundance of caution.

What We Are Doing

We take this event and the security of personal information entrusted to us very seriously and have taken steps to help mitigate the potential for harm and prevent this from happening again. After discovering the incident, we reset account passwords for all logins to affected KMJ email accounts in order to enhance the existing protections on our email system. We reported the incident to law enforcement. We also partnered with computer forensics professionals to thoroughly investigate, commenced a review of the entire contents of the accounts, notified potentially affected individuals about it, and are now continuing to evaluate ways to strengthen the security of our network going forward.

As an added precaution to help protect your identity, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12/24 months>> of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

With this protection, IDX will help you resolve issues if your identity is compromised. More information on these services and how to take advantage of them may be found in the enclosed *Additional Steps to Help Protect Personal Information*.

What You Can Do

We encourage you to remain vigilant for incidents of fraud or misuse, from any source, by reviewing and monitoring your account statements and credit reports. We recommend you report errors or suspicious activity to your financial institution or issuing bank immediately. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. Please refer to the enclosed documentation which contains additional steps you may take to protect your information from misuse, should you find it appropriate to do so.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling **1-833-903-3648** or going to **https://app.idx.us/account-creation/protect** and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Please note the deadline to enroll is October 13, 2022.

For More Information

If you have any other questions or concerns, you may contact us at 1-833-903-3648 for further information and assistance. We are very sorry for any concern or inconvenience this incident has caused or may cause you, and we encourage you to take advantage of the resources we are offering you. KMJ remains committed to safeguarding the information in our care.

Sincerely,

Jim Nagengast
Tax Partner
KMJ Corbin & Company LLP

ADDITIONAL STEPS TO HELP PROTECT PERSONAL INFORMATION

Enroll in Identity Theft Protection Services through IDX.

1. Website and Enrollment. Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-903-3648 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-888-298-0045	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report suspected fraud. You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place a Fraud Alert. Consumers have the right to place a fraud alert on their credit file at no cost. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Initial fraud alerts are for one year and identity theft victims can get an extended fraud alert for up to seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a fraud alert, contact the nationwide consumer reporting agencies by phone or online using the above contact information. For more information about placing a fraud alert, please visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide consumer reporting agencies by phone or online using the contact information above. If you request a freeze online or by phone, the agency must place the freeze within one business day. For more information, about placing a security freeze,

please visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **District of Columbia Residents:** District of Columbia Attorney General may be contacted at 400 6th Street NW, Washington D.C. 20001, and (202) 727-3400.
- **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division may be contacted at 200 St. Paul Place, 16th Flr., Baltimore, MD 21202, www.oag.state.md.us/Consumer, and toll-free at (888) 743-0023 or (410) 528-8662.
- **New York Residents:** New York Attorney General may be contacted at Office of Attorney General, The Capitol, Albany, NY 12224-0341, https://ag.ny.gov, and (800) 771-7755.
- **North Carolina Residents:** Office of the Attorney General of North Carolina may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, https://ncdoj.com, and (919) 716-6400.
- **All U.S. Residents:** The Identity Theft Clearinghouse, Federal Trade Commission may be contacted at 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, and 1-877-IDTHEFT (438-4338). This notification has not been delayed by law enforcement.

Know Your Rights Under the Fair Credit Reporting Act. You have certain rights pursuant to the Federal Fair Credit Reporting Act (FCRA) which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. You can read more by visiting https://consumer.ftc.gov/articles/ 0070-credit-your-consumer-rights and https://consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0070-credit-and-your-consumer-rights_1.pdf. These rights include: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (you "file disclosure"); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (8) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (9) You may seek damages from violators; and (10) identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit. States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.