Eva J. Pulliam
Partner
202.857.6323 DIRECT
202.857.6395 FAX
eva.pulliam@arentfox.com

January 7, 2021

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

Dear Sir or Madam:

My name is Eva Pulliam and I am a Partner at Arent Fox LLP. We represent KIND LLC. We are reaching out to you to provide information regarding a data incident experienced by KIND's vendor, Fiondella, Milone & LaSaracina LLP (FML). FML reported that its systems, including its systems holding KIND's employee personal data, were subject to an incident. Although FML has already provided notice of the incident to your office, KIND is separately providing notification to provide details about how KIND personal data has been impacted in FML's incident. KIND is providing notice after receiving information from FML about the scope of the incident and the specific impact to KIND personal data.

We provide details of the incident based on reports that we received from FML. According to FML, on September 14, 2021, FML identified unusual system activity on its network. FML promptly took steps to respond and to commence an investigation into the activity. FML's investigation determined that it was the target of a cyber-attack that impacted its network from September 9 to 14, 2021. The investigation further found that certain folders were potentially copied but could not confirm exactly which documents and data were copied. At this time, we know that FML's affected systems included personal information such as names and social security numbers.

Protecting the privacy and security of data is of critical importance to KIND. KIND has been actively working to investigate whether KIND information was actually compromised and has received further information about FML's full investigation of the incident, which was conducted with the support of cybersecurity and privacy experts. KIND has received information that FML has put in place additional security controls to protect against future attacks and further incidents. FML is reviewing and enhancing existing policies and procedures and implementing additional safeguards to further secure the information in its systems. KIND has been informed that the full functionality of all FML systems has been restored.

FML will be sending out a notice letter with a free credit monitoring offer to affected individuals shortly, and KIND will also be sending out its own notice. KIND's notice to affected individuals has gone out January 7, 2022 to two New Hampshire residents.

Please let us know if you have any questions or need anything further. We can be reached through email or phone at any time if there are any questions.

Regards,

Eva. J Pulliam

Enclosure

Laura J. Protzmann
Vice President, Deputy General Counsel
3 Times Square, 12th Floor
New York, NY 10036
O 212.616.3006 x 348
lprotzmann@kindsnacks.com

January 7, 2022

Notice of Data Incident

Dear Team Member:

We're writing to you as a valued current or former Team Member of KIND to inform you of a cybersecurity incident that affected one of our service providers and possibly your Team Member data. We are providing notice to you about this incident because we care about your privacy. Further information about the incident and credit monitoring services is forthcoming in a letter to be mailed to you from the service provider, Fiondella, Milone & LaSaracina LLP ("FML"), a sample of which is attached.

What Happened?	FML is a certified public accounting firm that provides tax and audit services to KIND. FML's systems, including its systems holding KIND Team Member data, were subject to an incident. On or about October 13, 2021, FML's investigation determined that certain folders on its network were potentially copied from its systems as part of a ransomware attack between September 9 and September 14, 2021. KIND became aware of the incident on November 8, 2021 and is providing this notice after receiving further information from FML about the incident.
What Information Was Involved?	At this time, we know that FML's affected systems included personal information such as Team Member names and social security numbers. FML's investigation determined that certain folders were potentially copied but could not confirm exactly which documents and data were copied, including whether KIND Team Member data was copied. FML's systems have since been restored.
What are We Doing?	Protecting the privacy and security of your data is of critical importance to KIND. KIND has been actively working to investigate whether KIND information was actually compromised and has received further information about FML's full investigation of the incident, which was conducted with the support of cybersecurity and privacy experts. FML has put in place additional security controls to protect against future attacks and further incidents. Though there is no confirmation that your personal information was taken, KIND is informing you of this incident because we respect your privacy.
What You Can Do.	As a precautionary measure, we encourage you to remain alert to monitor for misuse of your personal information. It is always good practice to monitor your account statements and credit reports to guard against fraud and identity theft. The forthcoming notice letter from FML contains information and instructions for credit monitoring services at no cost to you. It also contains information on contacting credit reporting agencies, placing a credit freeze, placing a fraud alert,

	contacting the Federal Trade Commission, and more steps you can take to protect your personal information.
For More Information	For more information, please carefully review the sample letter from FML attached. If you have additional questions or concerns, FML has established a dedicated assistance call center line at 855-604-1655, which is available Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time. You may also contact privacy@kindsnacks.com.

Sincerely,

Laura J. Protzmann

SAMPLE NOTICE LETTER FROM FML

<<Return Mail Address>> <<Date>>

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

RE: Notice of Data [Incident/Breach]

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

Fiondella, Milone & LaSaracina LLP ("FML") is writing to make you aware of a recent incident that may impact some of your information. FML is a Certified Public Accounting firm that provides tax and audit services. We have your information because we provided tax, audit or accounting services to you individually or a company with which you may be associated. This notice provides you with information about the incident, our response, and steps you may take to help protect your personal information, should you feel it is appropriate to do so.

What Happened? On September 14, 2021, FML identified unusual system activity on our network. We promptly took steps to respond and to commence an investigation into the activity. Through the initial investigation, we determined that FML was the target of a cyber-attack that impacted our network. We took steps to secure our systems and undertook a comprehensive investigation to confirm the full nature and scope of the event. On or about October 13, 2021, the investigation determined that certain folders on our network were potentially copied from our systems as part of the cyberattack between September 9 and September 14, 2021. While the investigation could not confirm exactly which documents were copied, in an abundance of caution, we are undertaking a comprehensive review of the potentially impacted folders in order to identify the information that was present and to whom it related.

What Information Was Involved? While the review is ongoing, based on our investigation to date, we determined that your information was present in the relevant folders. The data included your name and Social Security number.

What We Are Doing. Information security is one of FML's highest priorities, and we have security measures in place to protect information in our care. We responded promptly when we discovered this incident by taking steps to secure our systems and commence a comprehensive investigation. We are also reviewing and enhancing existing policies and procedures and implementing additional safeguards to further secure the information in our systems in the future. We reported this incident to federal law enforcement and are also notifying relevant regulatory authorities.

As an added precaution, FML is offering you access to [x] months of credit monitoring and identity protection services at no cost to you. You will find information on how to enroll in these services in the enclosed "*Steps You*

Can Take To Help Protect Your Information." We encourage you to enroll in these services as we are not able to do so on your behalf.

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 information contained in the attached "*Steps You Can Take To Help Protect Your Information*."

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or concerns, please call our dedicated assistance line at 855-604-1655, which is available Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time. You may also write to FML at 300 Winding Brook Drive, Glastonbury, CT 06033. Please know we take this incident very seriously and sincerely regret any inconvenience or concern it may cause you.

Sincerely,

Fiondella, Milone & LaSaracina LLP

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enroll in Credit Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for [x] months.

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 from the date of the incident (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 Identity Restoration is available to you for [x] months 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [x]-month 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** [Enrollment End Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code**: [Activation Code]

If you have questions about the product, need assistance with Identity Restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 994-0283 by [Enrollment End Date]. Be prepared to provide engagement number [DB#####] as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [x]-MONTH EXPERIAN IDENTITYWORKS 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™:** 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.

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 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, 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 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

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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and 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.

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 violator. 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, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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/.

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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 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 known Rhode Island residents potentially impacted by this incident.