MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Edward J. Finn
Office: (267) 930-4776
Fax: (267) 930-4771
Email: efinn@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

March 11, 2021

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 Kitestring Consulting, Inc. ("Kitestring"), located at 908 S Walton Blvd. #32, Bentonville, AR, 72712, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Kitestring 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

Kitestring utilizes a payroll processing vendor that stores data for accounting and payroll systems. On February 1, 2021, Kitestring became aware of suspicious activity relating to Kitestring data that is hosted by that vendor and immediately launched an investigation to determine the nature and scope of the activity. Kitestring determined that an unauthorized actor gained access to the vendor's server that housed Kitestring data and reports and attempted to encrypt certain files.

Despite a thorough investigation, Kitestring was unable to determine whether any information on the server was actually viewed or accessed by the unauthorized actor; however, the investigation could not rule out the possibility of such activity. Therefore, in an abundance of caution, Kitestring undertook a review of the files that were on the systems.

This review was recently completed, and it was determined that information relating to individuals was present on the impacted system that was hosted by a third-party provider.

The information that could have been subject to unauthorized access includes name, address, Social Security number, driver's license number, and bank account information.

Notice to New Hampshire Resident

On or about March 11, 2021, Kitestring began providing written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. 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

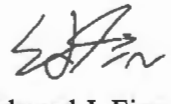
Upon discovering the event, Kitestring moved quickly to investigate and respond to the incident, assess the security of Kitestring systems, and notify potentially affected individuals. Kitestring is also working to evaluate policies with its vendors and implement additional safeguards. Kitestring is providing access to credit monitoring services for one (1) year, through Kroll, to individuals whose information was potentially affected by this incident, at no cost to these individuals.

Additionally, Kitestring is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Kitestring is 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,



Edward J. Finn of
MULLEN COUGHLIN LLC

EJF/zlg
Enclosure

EXHIBIT A

KITE STRING

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Kitestring Consulting, Inc. ("Kitestring") is writing to notify you of a recent incident that may have impacted some of your information. Although at this time there is no indication that your information has been misused in relation to this incident, we are providing you with information about the incident, our response to it, and additional measures you can take to better protect your information, should you feel it appropriate to do so.

What Happened? As part of Kitestring's payroll processing, we utilize a vendor that specializes in storing data for accounting and payroll systems. On February 1, 2021, Kitestring became aware of suspicious activity relating to our data that is hosted by the vendor, and immediately launched an investigation to determine the nature and scope of the activity. Kitestring determined that an unauthorized actor gained access to the vendor's server that housed Kitestring data and reports and attempted to encrypt certain files. This incident was not connected to any of Kitestring's in-house servers or data storage and only impacted the third-party server that housed Kitestring payroll data.

Unfortunately, despite a thorough investigation we were unable to determine whether any information on the server was actually viewed or accessed by the unauthorized actor; however, we could not rule out the possibility of such activity. In an abundance of caution, Kitestring undertook a review of the files that were on the systems. This review was recently completed, and it was determined that information related to you was contained on an impacted system that was hosted by a third-party provider.

What Information Was Involved? In order to process payroll and related taxes, Kitestring is required to store certain employee information. Our review of the files determined that your <<b2b_text_1(DataElements)>> were present on the impacted third-party server. Kitestring has not received any reports of misuse of any information relating to this incident.

What We Are Doing. The confidentiality, privacy, and security of your information are among our highest priorities, and we have strict security measures in place to protect information in our care. Upon learning of this incident, we immediately took steps to secure the vendor's systems and investigate the incident.

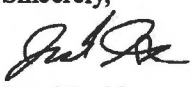
While we are unaware of any misuse of your information as a result of this incident, as an additional precaution, Kitestring is offering you access to twelve (12) months of complimentary identity monitoring services through Kroll. Details of this offer and instructions on how to activate these services are enclosed with this letter.

What Can You Do? Please review the enclosed document, "Steps You Can Take to Help Protect Your Information," which contains information on what you can do to safeguard against possible misuse of your information. You can also activate in the identity monitoring services that Kitestring is offering to you.

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 toll-free dedicated assistance line at 1-XXX-XXX-XXXX. This toll-free line is available Monday – Friday from 9:00 am ET until 6:30 pm ET, excluding some U.S. holidays.

Sincerely,



Jared Smith
President and CEO

Steps You Can Take to Help Protect Your Information

Activate Your Identity Monitoring

Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. To activate:

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **June 7, 2021** to activate your identity monitoring*

Membership Number: **<<Member ID>>**

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

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, military identification, 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 fraud alert or 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 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. Kitestring is located at 908 S. Walton Boulevard, #32, Bentonville, AR 72712.

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.