Fisher Broyles

Tony Onorato, Esq./CIPP(US)
New York Office

445 Park Avenue, Ninth Floor
New York, NY 10022

October 30, 2023

Via email to DOJ-CPB@doj.nh.gov
Attorney General John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Data Incident Concerning LiveAction, Inc.

Dear Office of the Attorney General:

This firm represents LiveAction, Inc. ("LiveAction"), a software company that provides simple real-time analytics, network monitoring and application performance management tools, located at 901 Campisi Way, Suite 222, Campbell, CA 95008. We write to inform your office of a recent IT incident, described in more detail below. LiveAction takes the security and privacy of the information in its control seriously and has taken steps to prevent a similar incident from occurring in the future.

I. Description of the Incident

On or about May 22, 2023, LiveAction detected and stopped a sophisticated ransomware attack, in which an unauthorized third party accessed and disabled some of LiveAction's computer systems. LiveAction immediately initiated its response protocols, launched an investigation, engaged a national cybersecurity firm to assist in assessing the scope of the incident, contacted the Federal Bureau of Investigation and took steps to mitigate the potential impact to its employees and business partners.

Upon detecting this incident, LiveAction moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of its network environment. LiveAction wiped and rebuilt affected systems and took steps to bolster its network security and is increasing the frequency of employee training. In addition, it reviewed and altered its policies, procedures, and network security software relating to the security of its systems and servers, as well as how it stores and manages data.

Since becoming aware of the unauthorized access, LiveAction has worked diligently to determine what happened and what information was potentially involved as a result of this incident.

As of this writing, LiveAction has not received any reports of fraud or identity theft related to this matter. However, elements of personal information that may have been compromised included:

.

II. Number of Residents Affected.

LiveAction discovered that the incident may have resulted in the exposure of information pertaining to six (6) New Hampshire residents. Notification letters to these individuals were mailed on September 27, 2023 via First Class Mail. A sample of the notification letter sent to affected residents is submitted herewith.

III. Steps Taken.

LiveAction takes the security of sensitive information that its customers entrust in it very seriously. Upon detecting this incident, LiveAction moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of its network environment. LiveAction wiped and rebuilt affected systems and took steps to bolster its network security. In addition, it reviewed and altered its policies, procedures, and network security software relating to the security of its systems and servers, as well as how it stores and manages data.

Additionally, the notified New Hampshire residents whose personal information were potentially compromised were offered complimentary identity theft and credit monitoring services provided by Kroll for .

IV. Contact Information.

LiveAction remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at .

Sincerely,

Tony Onorato
Partner, FisherBroyles, LLP

LiveAction

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

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

Notice of Data Incident

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

LiveAction is a software company that provides simple real-time analytics, network monitoring and application performance management tools. We are writing to inform you of a cyber incident which may have affected your personal information. We take the security of your information seriously and want to provide you with information and resources you can use to help protect your information.

At present, there is no evidence that any of your personal information has been misused; however, out of an abundance of caution, we are notifying you of this incident and offering you the resources discussed below so that you can take precautionary steps to help protect yourself, should you wish to do so.

What Happened

On or about May 22, 2023, we detected and stopped a sophisticated ransomware attack, in which an unauthorized third party accessed and disabled some of LiveAction's computer systems. We immediately initiated our response protocols, launched an investigation, engaged a national cybersecurity firm to assist in assessing the scope of the incident, contacted the US FBI and took steps to mitigate the potential impact to our employees and business partners.

Unfortunately, these types of incidents are becoming increasingly common and even organizations with some of the most sophisticated IT infrastructure available are affected. You are now receiving this letter because we have been working diligently to determine what happened and what information was involved as a result of this incident. Accordingly, we engaged a third-party to review the information that may have been impacted. This review was comprehensive and time consuming.

What Information Was Involved

At present, there is no evidence that any of your personal information has been misused; however, elements of your personal information that may have been compromised included your:

What We Are Doing

Data security is one of our highest priorities. Upon detecting this incident we moved quickly to initiate a response, which included conducting an investigation with the assistance of IT specialists and confirming the security of our network environment. We wiped and rebuilt affected systems and have taken steps to bolster our network security. We also reviewed and altered our policies, procedures, and network security software relating to the security of our systems and servers, as well as how we store and manage data.

We value the safety of your personal information and we want to make sure you have the information you need so that you can take steps to help protect yourself from identity theft. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps below.

What You Can Do

Complimentary Identity Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

KROLL

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.

Additional Steps

In addition to activating in the complimentary identity monitoring services being offered, we encourage you to review the enclosed *Steps You Can Take to Help Protect Your Information* for additional information on how to help protect against identify theft and fraud.

For More Information

On behalf of LiveAction, please accept my sincere apology for this isolated incident and any inconvenience it may cause you. LiveAction values its relationship with its employees, business partners and others who provide us with information.

I can assure you that we are taking steps intended to prevent an incident like this from reoccurring and helping to protect you and your information, now and in the future.

If you have questions, please call 1-???-???-????, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

LiveAction

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia,* and *Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon,* and *West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of *Washington, D.C.*: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of *Maryland, Rhode Island, Illinois, New York,* and *North Carolina*: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts and Rhode Island*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348 equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013 experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.