HOGE ▪ FENTON

Stephanie O. Sparks
408.947.2431
stephanie.sparks@hogefenton.com

August 14, 2023

Via Electronic Mail and First-Class U.S. Mail

Office of the Attorney General of Maryland
Anthony G. Brown
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: IDtheft@oag.state.md.us

Re: KP LLC Security Incident

Dear Sir or Madam:

We are writing on behalf of our client, KP LLC ("KP") regarding a security incident. Early on April 13, 2023, KP was alerted to suspicious activity on its systems. KP immediately implemented its incident response plan and engaged a leading cybersecurity firm to investigate the incident. KP notified federal law enforcement, a complaint was filed with the Federal Bureau of Investigation ("FBI") Internet Crime Complaint Center (www.ic3.gov), and KP has and will continue to cooperate with law enforcement investigations.

Based on the forensic investigation, the cybersecurity firm determined that initial unauthorized access to KP's network occurred on April 2, 2023, during the few hours when a Fortinet firewall was down one patch level during an infrastructure change. KP has taken several steps to contain the incident and enhance its security including changing passwords and using a managed detection and response ("MDR") service, which is monitored and actioned upon 24/7/365 by a third-party security operations center ("SOC").

The forensic investigation also discovered unauthorized access to certain internal servers that store KP business administration information. KP analyzed the servers impacted and recently determined that HR files containing personal information of current and former employees (collectively, "employees") were compromised.

From KP's analysis, there was one (1) Maryland resident impacted by the incident. Notification to that individual will be mailed on or about August 15, 2023. A sample of that notification is enclosed. Though KP does not have evidence that any personal information has been fraudulently used as a result of the incident, KP is offering impacted individuals two (2) years of free identity monitoring services, including credit monitoring, fraud consultation and identity theft restoration services through Kroll. In addition, in its written notification, KP provides impacted individuals detailed information and steps they can take to protect themselves and their personal information.

KP takes this incident, and the privacy and security of personal information, very seriously. If you have any questions or require further information, please feel free to contact me at stephanie.sparks@hogefenton.com or (408) 947-2431.

Very truly yours,

HOGE, FENTON, JONES & APPEL, INC.

Stephanie O. Sparks

Stephanie O. Sparks
Shareholder

SOS:ss
Encl.

KP

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

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

Re: Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to let you know about a security incident involving certain of your personal information. This notice explains what happened, what information may have been affected, what measures we are taking in response, and steps you can take to help protect yourself.

What Happened

On April 13, 2023, we experienced suspicious activity on our network at KP. We immediately implemented our incident response plan and engaged a leading cybersecurity forensics firm to investigate the incident. We notified law enforcement and filed a complaint with the U.S. Federal Bureau of Investigation ("FBI") Internet Crime Complaint Center. We took measures to contain the incident, including changing passwords and using a managed detection and response ("MDR") service, which is monitored and actioned upon 24/7/365 by a third-party security operations center.

Based on the forensic investigation to date, it appears that an unknown third-party gained unauthorized access to internal servers at KP that store business administration information. Following an analysis of the servers impacted, we recently determined that HR files containing certain of your personal information were exposed during the incident. Below, we describe what information was involved, what we are doing in response to the incident, and what you can do to be proactive and help protect yourself.

What Information Was Involved

One of the impacted servers stored employee records, including your name, address, email address, phone number, social security number, driver's license, passport or other government identification numbers, and date of birth. We do not store your credit card or other financial information, nor do we store your health or medical records.

What We Are Doing

As noted above, as soon as we discovered the suspicious activity, we immediately implemented our incident response plan, notified law enforcement, and engaged a leading forensics firm to investigate the incident. We took steps to contain the incident and further enhance the security of our systems, including changing passwords and installing endpoint detection sensors on devices, which are monitored 24/7/365 by a third-party security operations center.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you for two years. 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 Single Bureau 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.

What You Can Do

Please review the enclosed “Additional Resources” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call xxx-xxx-xxxx, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to the security of your information.

Sincerely,

B Olszewski

Brett Olszewski
CEO
KP LLC

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Maryland, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

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 help 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.