Clark Hill

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email:mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

July 6, 2022

VIA ELECTRONIC MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202
IDtheft@oag.state.md.us

To Whom It May Concern:

We represent InnerWorkings, Inc. ("InnerWorkings") with respect to a data security incident involving the potential exposure of personally identifiable information described in more detail below. InnerWorkings takes the security of information in its control seriously and has taken steps to prevent a similar incident in the future.

1. Nature of security incident.

On September 30, 2021, InnerWorkings identified suspicious activity on a limited number of servers located in the United States. InnerWorkings began an internal investigation and determined that they had suffered a ransomware attack. InnerWorkings immediately implemented its incident response protocols and engaged an independent computer forensic firm to assist in responding to and investigating this incident. The investigation found that personal information was stored on portions of the system affected by the incident but was unable to determine which information, specifically, may have been compromised. Thus, out of an abundance of caution, InnerWorkings is notifying all former and current employees in writing about the incident. Information present on the server at the time of the incident includes current and former employee names, addresses, Social Security numbers, driver's license numbers, and other HR related information.

2. Number of residents affected.

Thirty-two (32) residents of Maryland were notified of the incident. A notification letter was sent to the affected individual(s) on July 6, 2022 via regular mail. A copy of the form notification letter is enclosed with this communication.

3. Steps taken relating to the incident.

In response to the incident, access to certain servers within the environment were temporarily disconnected and CyLR, an endpoint protection software, was deployed on all systems. Independent computer forensic experts were engaged to assist with determining the scope and impact of the incident. Critical systems were restored, and InnerWorkings is continuously reviewing its security posture to ensure appropriate controls are in place. Impacted individuals were also offered 12 months of credit monitoring and identity protection services through Equifax.

4. Contact Information.

InnerWorkings remains dedicated to protecting the confidential information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Very truly yours,

CLARK HILL

Melissa K. Ventrone

Enclosure

HH Global
203 N La Salle St
Suite 1800
Chicago, IL 60601

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

<Date>

Notice of Data Security Incident

Dear <First Name> <Last Name>:

We are writing to inform you of a recent data security incident experienced by InnerWorkings, Inc. ("InnerWorkings") that may have impacted your personal information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

What Happened:

On September 30, 2021, InnerWorkings identified suspicious activity on a limited number of servers located in the United States. InnerWorkings began an internal investigation and determined that they had suffered a ransomware attack. InnerWorkings immediately implemented its incident response protocols and engaged an independent computer forensic firm to assist in responding to and investigating this incident. The investigation found that your information was stored on portions of the system affected by the incident but was unable to determine whether your information was compromised. Thus, we wanted to notify you of this incident out of an abundance of caution.

What Information Was Involved:

The information stored in the system could have included a combination of the following: your name, date of birth, driver's license number, passport number, mailing address, and Social Security number.

What We Are Doing:

We want to assure you that we are taking steps to minimize the risk of this kind of event from happening in the future. In response to the incident, access to certain servers within the environment were temporarily disconnected and endpoint protection software was deployed on all systems. Independent computer forensic experts were engaged to assist with determining the scope and impact of the incident. And we have arranged for you to receive **<Term>** of credit monitoring services offered by Equifax at no cost to you. Equifax services include credit monitoring with email notifications of key changes to your Equifax credit report, daily access to your Equifax credit report, WebScan notifications when your personal information, such as Social Security number, credit/debit card or bank account numbers are

found on fraudulent internet trading sites, automatic fraud alerts, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock, identity restoration to help restore your identity should you become a victim of identity theft, a dedicated identity restoration specialist to work on your behalf, and up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft.

What You Can Do:

At this time, there is no evidence that your information was misused. That said, it is always a good idea to review your credit report to identify any suspicious activity.

We encourage you to enroll in free Equifax identity protection services by going to **www.equifax.com/activate** More information on how to enroll is provided below. Please note that the **deadline to enroll in these services is September 30, 2022**.

For More Information:

Please contact hr.notification@hhglobal.com or the address listed at the top of this letter with any questions. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Innerworkings, Inc.

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. **Website and Enrollment.** Go to **www.equifax.com/activate** and follow the instructions for enrollment using your unique Activation Code of **<Activation Code>** then click "Submit." To register, complete the form with your contact information and click "Continue". If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page. To create your account, enter your email address, create a password, and accept the terms of use. To enroll in your product, Equifax will ask you to complete their identity verification process. Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. Click "View My Product" to access the product features.

2. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. 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 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

You should also know that 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 can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

3. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-836-6351
www.equifax.com/personal/credit-report-services

Experian Fraud Reporting and Credit Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion Fraud Reporting
P.O. Box 2000
Chester, PA 19022-2000

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094
1-800-680-7289
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

4. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

5. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

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

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 agencies 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 a 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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201904_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.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. You have the right to obtain any police report filed in regard to this incident. There is 1 Rhode Island resident impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.