Clark Hill

CONSUMER PROTECTION DIVISION
MAR 11 2022
OFFICE OF THE ATTORNEY GENERAL

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

March 4, 2022

Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

We represent Ziegler Metzger, LLP ("Ziegler") with respect to a data security incident involving potential exposure of certain personally identifiable information ("PII") in more detail below. Ziegler is a full-service law firm located in Cleveland, Ohio. Ziegler is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On July 26, 2021, Ziegler observed suspicious activities within its email environment. Ziegler immediately began an investigation and engaged external cybersecurity experts to conduct a forensic investigation to determine how the incident occurred and what information may have been impacted.

The investigation found that the unauthorized activities were limited to one employee's email account and the searching of that employee email account took quite a bit of time. As soon as Ziegler learned of this incident, Ziegler engaged independent cybersecurity experts to help determine what occurred, and what information may be at risk. Ziegler then had to obtain the contact information for impacted individuals and arrange for identity protection services at no cost to impacted individuals. This process took time to complete to ensure we have the most accurate information and contact for affected individuals.

The investigation is complete and Ziegler has determined that some client's personally identifiable information ("PII") may have been compromised as part of this incident. The investigation determined that the files impacted may have contained name, date of birth, Social Security number, driver's license number, address, and financial account information.

2. Number of residents affected.

One (1) Maryland resident may have been affected and was notified of the incident. A notification letter was sent to the potentially affected individuals on March 4, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

3. Steps taken in response to the incident.

Ziegler took steps to address this incident and to prevent similar incidents in the future, including changing passwords and retraining staff on the proper protocol in handling suspicious emails.

On March 4, 2022, Ziegler provided affected individual notice of this incident and was offered 12 months of credit monitoring and identity protection services through Cyberscout.

4. Contact information.

Ziegler takes the security of the information in its control seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at jschwent@clarkhill.com or (312) 985-5939.

Sincerely,

CLARK HILL

Jason Schwent
Senior Counsel

cc: Daisy Dai ddai@clarkhill.com

<Return Name>
<Return Address>
<City> <State> <Zip>

ZM | ZIEGLER METZGER LLP
ATTORNEYS AND COUNSELORS

<FirstName> <LastName>
<Address1>
<Address2>
<City><State><Zip>

March X, 2022

Notice of Data Security Incident

Dear <first name> <last name>:

We are writing to inform you of a data security incident experienced by Ziegler Metzger, LLP ("Ziegler") that may have impacted a limited amount of your personally identifiable information ("PII") described in more detail below. 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 July 26, 2021, one of our employees observed suspicious activities within their Ziegler email account. Specifically, they observed unauthorized messages sent from their email account and unauthorized rules created that moved incoming emails to bypass the inbox. We immediately began an investigation to determine how the incident occurred, and what information was potentially impacted. We also engaged Clark Hill PLC ("Counsel") to assist in the investigation of this incident and at Counsel's direction, engaged a nationally-recognized, third-party computer forensics firm, Kivu, to further assist in the investigation.

The investigation found that the unauthorized activities were limited to one employee's email account and the searching of that employee email account took quite a bit of time. As soon as we learned of this incident, we engaged independent cybersecurity experts to help us determine what occurred, and what information may be at risk. We then had to obtain the contact information for impacted individuals and arrange for identity protection services at no cost to you. This process took time to complete to ensure we have the most accurate information and contact for you. Ultimately, the investigation found that your information was present in the affected email account during the relevant period that the unauthorized user had access.

What Information Was Involved:

The categories of PII present in the affected email account include your name, <<data elements>>.

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. We made immediate enhancements to our systems, security and practices, including training our staff and resetting password for all accounts.

In addition, we are providing you with access to the following Cyberscout services:

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday. Please call the help line 1-800-405-6108 and supply the fraud specialist with your unique code listed below. To extend these services, enrollment in the monitoring services described below is required.

Additionally, we are providing you with access to **Single Bureau Credit Monitoring*** services at no charge. These services provide you with alerts for <<length of service>> months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring* services at no charge, please log on to **https://www.myidmanager.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: **<CODE HERE.>** In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

What You Can Do:

It is always a good idea to remain vigilant for incidents of identity theft or fraud, and to review your bank account and other financial statements as well as your credit reports for suspicious activity. We also encourage you to contact Cyberscout with any questions and take full advantage of Cyberscout's service offering. Additional information about protecting your identity is included in this letter, 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 any questions or concerns, please call 1-800-405-6108 Monday through Friday from 8 am - 8 pm Eastern Time, except holidays. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

Stephen Bales
Managing Partner
Ziegler Metzger LLP

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

RECOMMENDED STEPS TO HELP PROTECT YOUR INFORMATION

1. 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.

2. 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.

3. 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.

4. 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..

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.