

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Hilary Higgins
hhiggins@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

September 21, 2022

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Kingswood US, LLC ("Kingswood US") located at 175 Country Club Drive, Bldg 400, Suite D, Stockbridge, GA 30281 and write to inform you of a recent data security incident. By providing this notice, Kingswood US does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On March 3, 2022, Kingswood US became aware of potential unauthorized access to the email account of one employee. Upon discovery, Kingswood US immediately reset the password for the affected account and began an internal investigation. Further, Kingswood US engaged third-party specialists to assist with a full forensic investigation. The investigation confirmed that two employee email accounts were subject to unauthorized access. On July 18, 2022, after a thorough investigation, it was determined that information related to one (1) Maryland resident was potentially impacted. The impacted information is limited to Social Security number and financial account information.

On September 21, 2022, Kingswood US sent written notice of this incident to the potentially impacted Maryland resident pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to individuals is substantially similar to the letter attached hereto as Exhibit "A."

Very truly yours,



Hilary Higgins, Esq.
CIPRIANI & WERNER, P.C.

Exhibit A



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

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

<<b2b_text_1(Data Header)>>

Dear <<First_Name>> <<Last_Name>>,

Kingswood US, LLC ("Kingswood US") writes to notify you of a recent incident that may have involved some of your personal information.

Kingswood US takes the privacy of information in its care seriously. At this time, there is no evidence to suggest that any of your information was misused. In an abundance of caution, we are providing you information about the incident, our response, and steps you can take to help protect your information if you feel it is necessary to do so.

What Happened:

On or around March 3, 2022, Kingswood US became aware of potential unauthorized access to an email account belonging to an employee. Upon discovery, Kingswood US engaged a third-party team of forensic investigators in order to determine the full nature and scope of the incident. Following a full and thorough investigation, it was confirmed two employee email accounts were subject to unauthorized access during this incident. Upon confirmation of the unauthorized access to the employee email accounts, Kingswood US immediately investigated whether the affected email accounts contained sensitive information pertaining to individuals. On July 18, 2022, following a thorough investigation, Kingswood US confirmed that a limited amount of personal information may have been accessed in connection with this incident.

At this time, there is no indication that your information has been actually viewed or misused. However, Kingswood US is providing this notification to you in an abundance of caution and so that you may take steps to help safeguard your information if you feel it is necessary to do so.

What Information Was Involved:

The potentially accessed information may have included your <<b2b_text_2(Data Elements)>>.

What We Are Doing:

Kingswood US has taken steps to address the incident and is committed to protecting personal information in its care. Upon learning of this incident, Kingswood US immediately took steps to secure its systems and to enhance the security of its network.

Identity Monitoring:

As an additional safeguard for your information, Kingswood arranged for you to activate, at no cost to you, in an online identity monitoring service for 12 months. Due to State and Federal privacy laws, Kingswood US cannot activate you directly. If you wish to take advantage of this complimentary identity monitoring service, you must activate yourself.

What You Can Do:

Sign up for Identity Monitoring Services – We encourage you to contact Kroll with any questions and to activate your free identity monitoring services, use Membership Number, <<MembershipNumber (S_N)>>, and follow the steps to receive your identity monitoring service online within minutes. Please note the deadline to activate is <<b2b_text_6(Activation Deadline)>>.

In addition to activating the complimentary identity monitoring service detailed within, Kingswood US recommends that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password and take additional steps to help protect your account and notify your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your State Attorney General. Please review the additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft.

For More Information:.

Should you have questions or concerns regarding this matter, please do not hesitate to call our dedicated line to address this incident 1-???-???-???, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. Holidays. Please have your membership number ready. You may also write us at 175 Country Club Drive, Bldg 400, Suite D, Stockbridge, GA 30281.

Kingswood US takes the security of information entrusted to our care very seriously. While it is regrettable this potential exposure occurred, please be assured we are taking appropriate actions to rectify the situation and prevent such incidents in the future.

Sincerely,

Michael Nessim

Chief Executive Officer

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring

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(ActivationDeadline)>>** to activate your identity monitoring services.

Membership Number: **<<MembershipNumber(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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); 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:

TransUnion

1-800-680-7289

www.transunion.com

Experian

1-888-397-3742

www.experian.com

Equifax

1-888-298-0045

www.equifax.com

TransUnion Fraud Alert

P.O. Box 2000

Chester, PA 19016-2000

Experian Fraud Alert

P.O. Box 9554

Allen, TX 75013

Equifax Fraud Alert

P.O. Box 105069

Atlanta, GA 30348-5069

TransUnion Credit Freeze

P.O. Box 160

Woodlyn, PA 19094

Experian Credit Freeze

P.O. Box 9554

Allen, TX 75013

Equifax Credit Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

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/201504_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

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



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.