CONSTANGY
BROOKS, SMITH &
PROPHETE LLP

August 11, 2023

VIA EMAIL: DOJ-CPB@doj.nh.gov

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Kinsley Group, Inc. ("Kinsley") in connection with a data security incident described in greater detail below.

1. **Nature of the security incident.**

On or about February 3, 2023, Kinsley discovered that it had experienced an incident disrupting access to certain of its systems. In response, Kinsley took immediate steps to secure its systems and promptly launched an investigation. In so doing, Kinsley engaged legal counsel to perform a privileged investigation to determine what happened and to identify any information that may have been accessed or acquired without authorization. On or about July 13, 2023, Kinsley determined that certain personal information relating to residents of New Hampshire may have been impacted, and then took steps to effectuate notification thereto as quickly as possible. Please note that Kinsley has no evidence of the misuse or attempted misuse of any potentially impacted information.

The information that may have been accessible by the malicious actor responsible for this incident includes potentially impacted individuals' names and Social Security number, or driver license number.

2. **Number of New Hampshire residents affected.**

Kinsley notified 8 New Hampshire residents of this incident via first class U.S. mail on August 11, 2023. A sample copy of the notification letter is included with this correspondence.

3. **Steps taken relating to the Incident.**

As soon as Kinsley discovered this incident, Kinsley launched an investigation to determine what happened and to identify the scope of potentially impacted information. In addition, Kinsley implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. Kinsley also notified the Federal Bureau of

Investigation of this incident and will provide whatever cooperation is necessary to hold the perpetrator(s) of the incident accountable.

Kinsley has established a toll-free call center through Cyberscout, a TransUnion company, to answer any questions about the incident and address related concerns. The call center is available at from 8:00 A.M. to 8:00 P.M. Eastern Time, Monday through Friday (excluding holidays). In addition, out of an abundance of caution, Kinsley is also providing complimentary credit monitoring and identity protection services to notified individuals.

4. Contact information.

Kinsley remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

James M. Paulino
Partner

Enclosure: Sample Notification Letter

Kinsley Group, Inc.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07655 8-4

[redacted]

August 11, 2023

Subject: Notice of Data Security Incident

[redacted],

I am writing to inform you of a recent data security incident experienced by Kinsley Group, Inc. ("Kinsley") that may have affected your personal information. Kinsley takes the privacy and security of all personal information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On February 3, 2023, Kinsley discovered that it had experienced an incident disrupting access to certain of its systems. In response, Kinsley took immediate steps to secure its systems and promptly launched an investigation. In so doing, Kinsley engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization. On July 13, 2023, Kinsley learned that your personal information may have been impacted in connection with the incident which is the reason for this notification. Please note that Kinsley has no evidence of the misuse or attempted misuse of any potentially impacted information.

What Information Was Involved? The information potentially impacted in connection with this incident included your .

What Are We Doing? As soon as Kinsley discovered this incident, Kinsley took the steps described above. In addition, Kinsley implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. Kinsley also notified the Federal Bureau of Investigation of this incident and will provide whatever cooperation is necessary to hold the perpetrator(s) of the incident accountable.

Although Kinsley has no evidence of the misuse of any potentially impacted information, Kinsley is providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity protection services at no charge to you. These services include Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. Kinsley also encourages you to enroll in the complementary services being offered to you. To enroll in Credit Monitoring and Identity Protection services at no charge to you, please log on to . and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within from the date of this letter. The enrollment requires 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.

You may also call Cyberscout, a TransUnion company, at . Representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please contact our dedicated call center for more information at , from 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays or please go to . You will need to reference the enrollment code above when calling or enrolling online, so please do not discard this letter.

Please accept my sincere apologies and know that Kinsley takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Kind regards,

Kurt Wiesel
Chief Financial Officer

The Kinsley Group | 14 Connecticut South Drive | East Granby, CT 06026

www.kinsley-group.com

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www riag ri.gov
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Kinsley Group, Inc.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-07655 8-4

KINSLEY
The Energy Solutions Company

[redacted]

August 11, 2023

Subject: Notice of Data Breach

[redacted],

I am writing to inform you of a recent data security incident experienced by Kinsley Group, Inc. ("Kinsley") that may have affected your personal information. Kinsley takes the privacy and security of all personal information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your personal information.

What Happened? On February 3, 2023, Kinsley discovered that it had experienced an incident disrupting access to certain of its systems. In response, Kinsley took immediate steps to secure its systems and promptly launched an investigation. In so doing, Kinsley engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization. On July 13, 2023, Kinsley learned that your personal information may have been impacted in connection with the incident which is the reason for this notification. Please note that Kinsley has no evidence of the misuse or attempted misuse of any potentially impacted information.

What Information Was Involved? The information potentially impacted in connection with this incident included your

What Are We Doing? As soon as Kinsley discovered this incident, Kinsley took the steps described above. In addition, Kinsley implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. Kinsley also notified the Federal Bureau of Investigation of this incident and will provide whatever cooperation is necessary to hold the perpetrator(s) of the incident accountable.

Although Kinsley has no evidence of the misuse of any potentially impacted information, Kinsley is providing you with information about steps that you can take to help protect your personal information and is offering you complimentary identity protection services at no charge to you. These services include Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. Kinsley also encourages you to enroll in the complementary services being offered to you. To enroll in Credit Monitoring and Identity Protection services at no charge to you, please log on to . and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

In order for you to receive the monitoring services described above, you must enroll within from the date of this letter. The enrollment requires 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.

You may also call Cyberscout, a TransUnion company, at Representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please contact our dedicated call center for more information at , from 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays or please go to . You will need to reference the enrollment code above when calling or enrolling online, so please do not discard this letter.

Please accept my sincere apologies and know that Kinsley takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Kind regards,

Kurt Wiesel
Chief Financial Officer

The Kinsley Group | 14 Connecticut South Drive | East Granby, CT 06026

www.kinsley-group.com

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www riag ri.gov
riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.