CONSTANGY
BROOKS, SMITH &
PROPHETE LLP

January 17, 2024

VIA EMAIL

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection & Antitrust Bureau
1 Granite Place South
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Arden Claims Service, LLC ("Arden"), a class action settlement administrator based in New York, in connection with the data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with New Hampshire's data breach notification statute.

1. **Nature of the Security Incident**

On or around October 17, 2023, Arden became aware of unusual activity related to an email account. In response, Arden took immediate steps to secure its email environment and promptly launched an investigation. The investigation conducted by the third-party cybersecurity experts determined that an unknown actor accessed and acquired certain data without authorization. Please note that the investigation into the scope of this incident is ongoing, and additional consumer and supplemental regulatory notification may be required at a later date.

On December 19, 2023, Arden confirmed that certain personal information may have been impacted and then took steps to effectuate notification to potentially impacted individuals as quickly as possible. Please note that there is currently no evidence of fraud or misuse of any of the data, only evidence that data was accessed or acquired without authorization.

2. **Number of Affected New Hampshire Residents & Information Involved**

The incident involved personal information for approximately seven (7) New Hampshire resident(s). The information involved in the incident for the affected New Hampshire resident(s) may have included .

3. Notification to Affected Individual(s)

On January 17, 2024, a notification letter was sent to the affected New Hampshire resident(s) by USPS First Class Mail. The notification letter provides resources and steps this individual can take to help protect their information. The notification letter also offers the individual whose Social Security number was affected by this event the opportunity to enroll in of complimentary identity protection services, including credit monitoring, dark web monitoring, $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. A sample notification letter sent to the impacted individual(s) is included with this correspondence.

4. Steps Taken Relating to the Incident

In response to the incident, Arden retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Arden also implemented additional security measures to further harden its email environment in an effort to prevent a similar event from occurring in the future. Additionally, Arden has reported the incident to the FBI and will cooperate with any resulting investigation.

Finally, Arden is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above. Arden has also established a toll-free call center through Cyberscout, a TransUnion company, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns.

5. Contact Information

Arden 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 Donna Maddux at

Best regards,

Donna Maddux
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Enclosure: Sample Notification Letter

Arden Claims Service, LLC
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

ARDEN CLAIMS SERVICE LLC
PROFESSIONAL • ACCOUNTABLE • RELIABLE

January 17, 2024

Re: Notice of Data Security Incident

Dear ,

Arden Claims Service LLC (Arden Claims Service) is writing to inform you of a data security incident that involved your personal information. Arden Claims Service is a class action settlement administrator and received your information in conjunction with related services. Arden Claims Service takes the privacy and security of your information very seriously. This is why we are notifying you of the incident, providing you with steps you can take to protect your information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On or around October 17, 2023, Arden became aware of unusual activity related to an email account. We immediately took steps to secure the account and engaged cybersecurity experts to conduct an investigation. The investigation determined that an unknown actor acquired certain data without authorization. After a thorough review of the impacted data, on December 19, 2023, it was determined that some of your personal information was present in the impacted data. We then took steps to notify you of the incident as quickly as possible.

What Information Was Involved? The data involved included

What We Are Doing: In addition to the steps described above, we implemented additional security measures to further protect our network and minimize the risk of future incidents. We also reported this incident to the Federal Bureau of Investigation.

We are also providing you with access to 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: We recommend that you review the guidance included with this letter about how to protect your information. To enroll in Credit Monitoring and Identity Protection services at no charge to you, please log on to **https://secure.identityforce.com/benefit/ardenclaimsserviceus** and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account. 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 1-833-573-2772. Representatives are available for 90 days from the date of this letter, Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays.

For More Information: If you have questions or need assistance, please contact our dedicated call center for more information at 1-833-573-2772, from 8:00 a.m. to 8:00 p.m. Eastern Time, Monday through Friday, excluding holidays or please go to **https://secure.identityforce.com/benefit/ardenclaimsserviceus**. Representatives are available for 90 days from the date of this letter. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

The privacy and security of personal information is a top priority for Arden Claims Service. We take this incident very seriously and regret any worry or inconvenience this may cause you.

Sincerely,

Barry Peek
Chief Executive Officer
Arden Claims Service, LLC
P.O. Box 1015
Port Washington, New York 11050

ADDITIONAL STEPS YOU CAN TAKE TO FURTHER 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 monitoring free credit reports closely for errors and by taking other steps appropriate to protect accounts, including promptly changing passwords. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained for remediation assistance or contact a remediation service provider. 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). You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the FTC is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Ave, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.consumer.ftc.gov, www.ftc.gov/idtheft.

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 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 can print this form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. You also can contact one of the following three national credit reporting agencies:

- *Equifax*, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285, www.equifax.com.
- *Experian*, P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com.
- *TransUnion*, P.O. Box 1000, Chester, PA 19016, 1-800-916-8800, www.transunion.com.

Fraud Alerts: There are two kinds of general fraud alerts you can place on your credit report—an initial alert and an extended alert. You may want to consider placing either or both fraud alerts on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and provide the appropriate documentary poof. An extended fraud alert is also free and will stay on your credit report for seven years. 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. Military members may also place an Active Duty Military Fraud Alert on their credit reports while deployed. An Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment

Credit or Security Freezes: Under U.S. law, you have the right to put a credit freeze, also known as a security freeze, on your credit file, for up to one year at no cost. The freeze 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. There is no fee to place or lift a security freeze. For information and instructions on how to place a security freeze, contact any of the credit reporting agencies or the FTC identified above. 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. After receiving your freeze request, each credit bureau will provide you with a unique PIN or password. Keep the PIN or password in a safe place as you will need it if you choose to lift the freeze.

A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or via phone, a credit bureau must lift the credit freeze within an hour. If the request is made by mail then the bureau must lift the freeze no later than three business days after receiving your request.

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include the right 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. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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.

Additional information:

Maryland: Maryland Attorney General can be reached at: 200 St. Paul Place Baltimore, MD 21202; 888-743-0023; oag@state.md.us or IDTheft@oag.state.md.us

New York: New York Attorney General can be reached at: Bureau of Internet and Technology Resources, 28 Liberty Street, New York, NY 10005; 212-416-8433; https://ag.ny.gov/

North Carolina: North Carolina Attorney General's Office, Consumer Protection Division, can be reached at: 9001 Mail Service Center Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov

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

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