David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, New York 11201
dmcmillan@constangy.com
Direct: 718.614.8371

May 8, 2024

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Office of Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: **Notice of Data Security Incident**

Dear Attorney General Frey:

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

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

On April 9, 2024, Ultrafab became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, Ultrafab immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. While that investigation is ongoing, Ultrafab has determined that an unauthorized actor accessed and acquired certain files stored in its network, some of which contained personal information for current and former Ultrafab employees. Following a review of those files, on April 25, 2024, Ultrafab confirmed that certain personal information was impacted and arranged to notify affected individuals as quickly as possible.

2. **Number of Maine residents affected.**

Ultrafab notified one (1) Maine resident of this incident via first class U.S. mail on May 8, 2024. The information potentially impacted in connection with this incident varies by individual but may include name, Social Security number, and driver's license number.

A sample copy of the notification letter is included with this correspondence.

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

As soon as Ultrafab discovered this incident, Ultrafab took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal and protected health information potentially impacted. In addition, Ultrafab implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future. Ultrafab also notified the Federal Bureau of Investigation.

Ultrafab has established a toll-free call center through Cyberscout, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while Ultrafab is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Ultrafab is also providing 24 months of complimentary credit and identity protection services to notified individuals whose Social Security numbers may have been impacted.

4. Contact information.

Ultrafab 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,

/s/ David McMillan

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter

Ultrafab, Inc.
c/o Cyberscout
1 Keystone Ave, Unit 700
Cherry Hill, NJ 08003
DB-08832 1-1

[redacted]

May 8, 2024

Subject: Notice of Data Security Incident:

Dear [redacted]:

We are writing to inform you of a data security incident experienced by Ultrafab, Inc. ("Ultrafab") that may have affected your personal information. Please read this letter carefully as it contains details about the incident and resources you can utilize to protect your information, including instructions for enrolling in complimentary credit monitoring and identity theft protection services.

What Happened? On April 9, 2024, Ultrafab became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, we immediately took steps to secure our network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. While that investigation is ongoing, we have determined that an unauthorized actor accessed and acquired certain files stored in our network, some of which contained personal information for current and former Ultrafab employees. On April 25, 2024 we determined that your information may have been impacted, and moved as quickly as possible to provide notice and resources to assist.

What Information Was Involved? The information involved this incident may have included your name Social Security number and driver's license.

What We Are Doing: As soon as we discovered this incident, we took immediate steps to secure our environment and enlisted a leading, independent cybersecurity firm to conduct a forensic investigation. We also reported the incident to the FBI and will cooperate with any resulting investigation. In addition, we have implemented several measures to enhance our network security and reduce the risk of similar future incidents.

We are also providing you with the opportunity to enroll in Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge to you. These services provide you with alerts for twenty-four months 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, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do: We encourage you to enroll in the credit monitoring and identity protection services we are offering, which are at no cost to you. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

To enroll in the credit monitoring and identity protection[1] services at no charge, please log on to https://bfs.cyberscout.com/activate and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. Please note you must enroll by August 6, 2024.

For More Information: 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 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the specialist with your unique code listed above.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Alan DeMello

Alan DeMello
President & CEO
Ultrafab, Inc.
1050 Hook Road
Farmington, NY 14425

[1] 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 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.

Steps You Can Take to Protect Your Personal 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).

Request a Copy of Your 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 https://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 105851
Atlanta, GA 30348
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

Place a 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 https://www.annualcreditreport.com.

Put a 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 (FTC)
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

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
1-401-274-4400

Washington D.C. Attorney General
441 4th 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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.