71 South Wacker Drive, Suite 1600
Chicago, IL 60606

June 8, 2023

New Hampshire Department of Justice
33 Capitol Street
Concord, NH 033301

By Email

RE: Headwall Photonics - Notice of Data Breach Incident

Attorney General Formella,

We are contacting you on behalf of our client, Headwall Photonics, Inc. of Bolton, Massachusetts regarding a recent security incident at the company. Our client is in the process of notifying the individuals, which included twenty-four affected New Hampshire residents. A template of the letter sent to the New Hampshire residents is attached for your review.

Below is a summary of the incident.

On May 26th while investigating a ransomware attack impacting Headwall's systems, Headwall discovered that the personal information of certain employees, former employees, investors, and businesses may have been compromised. Headwall discovered that the security of the personal data, including may have been compromised. Headwall responded promptly to this attack to mitigate the effects and restore Headwall's systems.

Additionally, Headwall has engaged with cybersecurity specialists and security experts and is in the process of reviewing and amending their security measures and protocols as needed. Headwall has also set up the affected individuals with free credit monitoring services.

Should you have any questions or concerns regarding this matter, please do not hesitate to contact me at

Sincerely,

Rachit Parikh

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP

Headwall

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

June 7, 2023

J5317-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

RE: Notice of Data Breach. Please read this entire letter.

Dear Sample A. Sample:

What Happened?	We are writing to inform you that Headwall Photonics ("Headwall") discovered a cybersecurity incident that may affect the security of your personal information.
What Information Was Involved?	The cybersecurity incident may have resulted in unauthorized access to your personal data. While investigating a ransomware attack experienced by Headwall, we discovered on May 26, 2023, that the security of your personal data which may include your name, address, passport number, driver's license number, and/or social security number ("Personal Data") may have been compromised. We responded promptly to this attack to end the attack and restore Headwall's systems; however, because of the potential unauthorized access to your Personal Data, there are measures that you may wish to take to protect yourself from the possibility of identity theft. We have described those measures below in this letter. In addition, we have procured free credit monitoring services for all affected individuals, such details are below.
What Are We Doing.	In light of the data breach, we are reviewing our security policies and procedures and will make updates as needed to better protect against future occurrences.
What You Can Do.	To protect yourself from the possibility of identity theft, we recommend that you immediately place a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other two on your behalf. You will then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each. Experian (888) 397-3742 or www.experian.com or P.O. Box 2104, Allen, TX 75013 Equifax (888) 766-0008 or https://www.equifax.com/ or P.O Box 740241, Atlanta, GA 30374 TransUnion (800) 680-7289 or www.transunion.com or P.O. Box 2000, Chester, PA 19016 When you receive a credit report from each agency, review the reports carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records.

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your credit reports from the three major credit reporting agencies and in reviewing your account statements. You may obtain a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228 or by completing an Annual Credit Request Form at: www ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing to:

Annual Credit Report Request Service,
P.O. Box 1025281
Atlanta, GA 30348-5283

For more information on identity theft, you can visit the following website:
- Federal Trade Commission at: www.ftc.gov/bcp/edu/microsites/idtheft/

Additionally, if you received correspondence or any communication from the Internal Revenue Service that you may have been a victim of tax-related identity theft or that your tax filing was rejected as a duplicate, you should immediately fill out a Form 14039 Identity Theft Affidavit and submit it to the Internal Revenue Service. You should continue to file your tax return, as applicable, and attach the Form 14039 Identity Theft Affidavit to the return. Tax-related identity theft occurs when someone uses a taxpayer's stolen Social Security number to file a tax return claiming a fraudulent refund.

For more information on when to file a Form 14039 Identity Theft Affidavit, you can visit the following website:

- Internal Revenue Service at: https://www.irs.gov/newsroom/when-to-file-an-identity-theft-affidavit

For more information on tax-related identity theft, you can visit the following website:

Internal Revenue Service at: https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for 24 months. This will be separate from the fraud alert you may put on your credit files, as explained above.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
- Provide your **activation code**:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at by September 30, 2023. Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

For More Information.	We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number . If there is anything that we can do to further assist you, please call, or email at

Additional State Specific Information

If you are a resident of Maryland:

- For more information on identity theft, you can visit or contact the Office of the Maryland Attorney General at the following:
  - Website: https://www.marylandattorneygeneral.gov/
  - Phone Number: 888-743-0023
  - Address: 200 St. Paul Place, Baltimore, MD 21202

If you are a resident of North Carolina:

- For more information on identity theft, you can visit or contact the Office of the North Carolina Attorney General at the following:
  - Website: https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id-theft/security-breach-information/
  - Phone number: 919-716-6000
  - Address: 114 West Edenton Street, Raleigh, NC 27603

If you are a resident of New York:

- For more information on identity theft, you can visit the following websites:
  - New York Department of State Division of Consumer Protection https://dos.nysits.acsitefactory.com/consumer-protection
  - NYS Attorney General at: http://www.ag.ny.gov/home.html
  - Phone Number: 800-771-7755

If you are a resident of Rhode Island:

- Rhode Island residents have the right to put a Security Freeze on their credit reports. A Security Freeze prevents most potential creditors from viewing your credit reports and therefore, further restricts the opening of unauthorized accounts. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. A separate Security Freeze must be requested and placed on the applicable credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a Security Freeze.

- Rhode Island residents also have the right to request and obtain a police report with regard to the data breach.

- For More Information on identity theft, you can visit or contact the Office of the Rhode Island Attorney General at the following:
    - Website: https://riag ri.gov/
    - Phone Number: 401-274-4400

Sincerely,

Leo Martin, Chief Financial Officer
Headwall Photonics