100 International Drive
23rd Floor
Baltimore, MD 21202

P 1.248.646.5070
F 1.248.646.5075

McDonald Hopkins
A business advisory and advocacy law firm®

Spencer S. Pollock, CIPP/US, CIPM
Direct Dial: (410) 456-2741
Cell: (410) 917-5189
E-mail: spollock@mcdonaldhopkins.com

October 13, 2023

VIA EMAIL (Idtheft@oag.state.md.us)

Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Peerstar LLC - Security Breach Notification

Dear Mr. Brown:

We are writing on behalf of our client, Peerstar LLC ("Peerstar") (located at 210 College Park Plaza Johnstown, PA 15904) to notify you of a data security incident involving nineteen (19) Maryland residents. By providing this notice, Peerstar does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

Nature

On or about March 7, 2023, Peerstar identified suspicious activity on its network associated with a potential ransomware incident. After discovering the incident, Peerstar engaged our firm and third-party independent cybersecurity experts to conduct a thorough investigation of the nature and scope of the incident and to assist in the remediation efforts.

Peerstar recently concluded its initial investigation, which revealed that an unauthorized actor gained access to Peerstar's systems, via a vulnerability, between February 22, 2023 to March 3, 2023, and as a result potentially obtained some information. On October 4, 2023, after an extensive forensic investigation and review, Peerstar discovered that certain personal information was included within the files that were subject to unauthorized access or acquisition as a result of the incident. Further, on October 12, 2023, Peerstar located the most recent contact information for these individuals. Peerstar determined that the incident involved nineteen (19) Maryland residents.

The personal information obtained potentially included first and last name in addition to one or more of the following data elements: address, phone number, email address, Social Security number, date of birth, admission date, discharge date, physical or mental health condition, treatment and diagnosis information, driver's license number or government-issued identification number, financial account number, credit or debit card number, digital signature, birth or marriage certificate, healthcare payment information, and/or health insurance information, including, application and claims history, and policy number or subscriber identification number. Not all data elements were impacted for all potentially affected individuals.

Notice and Peerstar's Response to the Event

On October 16, 2023, Peerstar will mail a written notification to the potentially affected Maryland residents, pursuant to Md. Code Ann., Com. Law § 14-3501-3508, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, Peerstar is providing the potentially impacted individuals the following:

- Free access to credit monitoring services for one year through TransUnion;

- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;

- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;

- A reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports; and

- Encouragement to contact the Federal Trade Commission and law enforcement to report attempted or actual identity theft and fraud.

Further, Peerstar provided notice to the applicable government regulators, officials, and other state Attorneys General (as necessary). Finally, Peerstar is working to implement any necessary additional safeguards; enhance and improve its policies and procedures related to data protection; improve its cybersecurity infrastructure; and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 456-2741 or email me at spollock@mcdonaldhopkins.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

PeerStar LLC
[redacted]

[redacted]

PEERSTAR LLC
A COMMUNITY BEHAVIORAL HEALTHCARE SERVICE
WORKING TOWARD RECOVERY AND INTEGRATION

P 00010102G0500

October 16, 2023

Re: Notice of a Data Notice of a Data Security Incident

Dear [redacted]

The privacy and security of the personal information we maintain is of the utmost importance to Peerstar, LLC. We're writing with important information regarding a recent data security incident that involved some of your information. We want to provide you with information about the incident, explain the services we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On March 7, 2023, we discovered suspicious activity on our network. After discovering this, we quickly took steps to evaluate and ensure the security of our systems and operations. Further, we immediately engaged third-party independent cybersecurity experts to conduct an investigation into the incident.

We recently concluded our initial investigation and determined that from February 22, 2023 to March 3, 2023, an unauthorized individual accessed our systems and, as a result, potentially obtained some information. At that time, we began a comprehensive review of the potentially impacted files, and on October 4, 2023, after an extensive forensic investigation and review, we discovered that certain personal information was included within the files that may have been accessed or removed from our network by an unauthorized actor as a result of the incident

We currently have no evidence indicating that any personal information has been used for identity theft or financial fraud as a result of the incident, however, out of an abundance of caution, we wanted to notify you of the incident and provide you with information on steps you can take to help protect your information.

What Information Was Involved?

The impacted files likely contained some of your personal or protected health information, specifically your [redacted] However, as stated above, we currently have no evidence indicating that as a result of this incident this information has been used for identity theft or financial fraud.

What We Are Doing.

The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we took immediate steps to secure our systems and engaged third-party forensic experts to assist in the investigation. Further, we are implementing additional cybersecurity safeguards, as needed, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

What You Can Do.

Finally, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for 12 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. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring services at no charge, please log on to [redacted] 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 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.

Additionally, if you are interested in learning about how you can contact the Federal Trade Commission and obtain information from credit reporting agencies about fraud alerts and security freezes, you may refer to the "Other Important Information” included with this letter.

For More Information.

Please accept our apologies that this incident occurred. We remain fully committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your personal information.

If you have any additional questions, please contact the external, dedicated call center we set up at [redacted] between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays.

Sincerely,

Peerstar LLC
210 College Park Plaza
Johnstown, PA 15904
[redacted]

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide 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 access the request form at https://www.annualcreditreport.com/index.action. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax	Experian	TransUnion
P.O. Box 105069 Atlanta, GA 30348-5069 https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ (800) 525-6285	P.O. Box 9554 Allen, TX 75013 https://www.experian.com/fraud/center.html (888) 397-3742	Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016-2000 https://www.transunion.com/fraud-alerts (800) 680-7289

Security Freeze (also known as a Credit Freeze). If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	Experian Security Freeze	TransUnion Security Freeze
P.O. Box 105788 Atlanta, GA 30348-5788 https://www.equifax.com/personal/credit-report-services/credit-freeze/ (888) 298-0045	P.O. Box 9554 Allen, TX 75013 http://experian.com/freeze (888) 397-3742	P.O. Box 160 Woodlyn, PA 19094 https://www.transunion.com/credit-freeze (888) 909-8872

Consider Placing a Fraud Alert on Your Credit Report. Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity.
As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft.
We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a

P 0000102028000

comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/.

Protecting Your Medical Information.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General’s Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, Telephone: 888-743-0023.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General’s Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General’s Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General’s Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

New Mexico Residents: Consumers have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the FCRA, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers’ files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit “prescreened” offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the FCRA not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. We encourage consumers to review their 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. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.