



Legal Counsel.

DINSMORE & SHOHL LLP
255 E. Fifth St., Suite 1900
Cincinnati, OH 45202
www.dinsmore.com

Gabrielle A. Hartstein
(330) 572-1956
gabrielle.hartstein@dinsmore.com

Barrett Eye Care
11450 N. Meridian St.
Suite 120
Carmel, IN 46032
(317) 872-8772

July 19, 2024

VIA EMAIL: Idtheft@oag.state.md.us

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

RE: Notice of Data Breach

To Whom It May Concern:

Dinsmore & Shohl LLP represents Barrett Eye Care ("Barrett"). Barrett operates an eye-care clinic offering high quality, comprehensive eye exams for routine and complicated eye diseases. I am writing to inform you of a recent security incident experienced by Barrett that may have potentially exposed personal information, including protected health information, relating to patients who received services from Barrett.

On June 2, 2024, Barrett Eye Care experienced a security incident where a threat actor gained unauthorized access to Barrett's systems, including the data stored on those systems. The threat actor used Lockbit Black Ransomware to send a ransom note, encrypt a server, and shut down the system. On June 4, 2024, Barrett discovered the attack and engaged legal counsel and a data breach remediation firm to conduct a thorough investigation into the scope of the illicit attack. Upon conducting an investigation, Barrett discovered that the majority of patient data on the impacted server was encrypted; however, there were unencrypted photos of Driver's License and Insurance Cards which when taken together contain both personal information and potentially PHI. These files were obscured by the fact that they did not provide a proper extension in the file name. To date, we have no evidence that these files were accessed. Barrett recognizes the *potential* that the files were accessed, and is providing notice out of an abundance of caution. The investigation is still

ongoing, but at the time of this notice, 1,694 individuals associated with Barrett were potentially affected one of which lives in Maryland. We foresee the potential to add more individuals to this list as our investigation progresses.

Barrett will provide affected individuals notice of the security incident via U.S. mail on July 19, 2024, which will include instructions on how to place a security freeze with the credit reporting agencies, a copy of which is attached. Additionally, Barrett has secured the services of Kroll, a data breach remediation service provider, to establish a call center to respond to any questions affected individuals may have about the cyberattack. A template copy of the individual data breach notification letter, along with instructions for how affected individuals can place and remove a security freeze, is enclosed with this letter.

If you have any additional questions or require more information, you can reach me by email at gabrielle.hartstein@dinsmore.com or by phone at (330) 572-1956.

Sincerely,

/s/ Gabrielle A. Hartstein

Gabrielle A. Hartstein

Enclosure



Barrett Eye Care
11450 North Meridian St.
Suite 120,
Carmel, IN 46032

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

July 19, 2024

RE: Important Security Notification. Please read this entire letter.

Dear Valued Patient:

We value and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a cyber security incident that occurred at our offices. Barrett Eye Care ("Barrett"), recently discovered a security incident that may affect the security of your personal information. This letter will provide you with information about the incident, steps we are taking in response, and steps you may take to guard against identity theft and fraud, should you feel it is appropriate to do so.

What Happened? On June 2, 2024, Barrett experienced a security incident where a threat actor gained unauthorized access to Barrett's systems, including the data stored on those systems. The incident allowed the threat actor to view and access certain personal information, while locking Barrett out of their own system. Although the threat actor was able to view and access personal information, there is no evidence, at the time of this letter, that the threat actor had taken these steps. The incident was discovered expeditiously, and proper security measures were conducted to contain the incident.

What Information Was Involved? The information subject to the incident may have included personal information such as your first name, last name, driver's license number and address along with health insurance information. Please note that you are receiving this notification because your personal information may have been exposed.

What Are We Doing? We take the protection of your personal information seriously and are taking steps to prevent a similar occurrence. Upon learning of the incident, Barrett took immediate measures to contain and neutralize the vulnerability, secure the IT environment, notify law enforcement, and initiate a forensic investigation to determine the extent of the incident. Barrett has also deployed, and will continue to deploy, additional security procedures to prevent future incidents. Finally, Barrett has engaged cyber security experts to guide us through the incident, ensuring that we fully comply with our legal obligations and properly mitigate the potential impact of the incident.

Barrett will continue to work with cyber security experts and law enforcement to ensure that this incident is properly addressed, ensure that we remain vigilant in the security of our own operations, and continue strengthen our internal controls and safeguards to ensure this type of incident does not occur again. Barrett will notify you of any significant developments that may further impact the security of your personal information.

What Actions You Can Take? As always, we recommend you be on the alert for suspicious activity related to your financial accounts and credit reports. We encourage you to regularly monitor your statements and records to ensure there are no transactions or other activities that you did not initiate or authorize. You should report any suspicious activity to the appropriate service provider.

We recommend that you obtain, and monitor, your credit reports to ensure that fraudulent activity has not occurred. In line with your rights pursuant to the federal Fair Credit Reporting Act, 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>, by 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.

Additionally, you should report incidents of suspected identity theft to your local law enforcement, the Federal Trade Commission, and your state attorney general. To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (1 (877) 438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Information on how to contact your state attorney general can be found below:

Attorney General Anthony G. Brown
200 St. Paul Place
Baltimore, MD 21202-2202
Main: (410) 576-6300
Consumer Hotline: (410) 528-8662
<https://www.marylandattorneygeneral.gov/Pages/contactus.aspx>

Please 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/privacyidentity-online-security>.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (1-877-438-4338). A copy of Identity Theft – A Recovery Plan, a 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/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Placing a Security Freeze

Any consumer in Maryland may place a security freeze on his or her credit report by requesting one in writing by certified mail to the consumer reporting agency. The consumer reporting agency is not allowed to charge a fee to victims for placing, removing for a specific period or party, or removing a security freeze on a credit report. To avoid a fee, the victim must also send a valid copy of a police report to the consumer reporting agency. However, for other consumers, a charge of \$5 will be applied for each placing, removing, or temporary lifting of a security freeze. This fee may be increased as the consumer price index rises. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. We recommend that you work collaboratively with potential lenders, employers and service providers to ensure that you are protecting both your information and the approval status of your applicable request.

In order to place a security freeze on your credit reports, you must contact all three bureaus and pay a fee to each, where applicable. For victims of identity theft, there are no fees. For all others, there is a \$5 fee every time you place, temporarily lift, or remove a security freeze. Your request to place a security freeze must be in the form of a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com), and sent by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
(888) 909-8872

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report, so we recommend placing the freeze as soon as you possibly can. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

Lifting or Suspending a Security Freeze

To temporarily lift or suspend the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report, or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities, or for the specified period of time.

Removing a Security Freeze

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call (866) 810-3352 toll-free Monday through Friday from 8 am – 5:30 pm Central (excluding major U.S. holidays).

Thank you for your immediate attention to this situation, as well as your understanding in the short-term. Our cyber security, as well as the safety and stability of our patients, employees, and vendors, is of the utmost importance to us and we remain committed to protecting your information. Again, we sincerely apologize for any impact caused by this incident. We will continue to monitor the incident and advise you of any updates as may be necessary.

Sincerely,

Dr. Erik Barrett, M.D.
Owner
Barrett Eye Care

