CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JOHN LOYAL
jloyal@c-wlaw.com

JORDAN MORGAN
jmorgan@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Telephone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

March 12, 2021

State of New Hampshire
Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03302

RE: Security Incident Notification

To Whom It May Concern:

I serve as counsel for Glaukos Corp. ("Glaukos") and provide this notification to you of a recent data security incident suffered by Glaukos. On or about October 9, 2020, Glaukos fell victim to a phishing attack as Glaukos employees were targeted with fraudulent emails containing a malicious link. Following an internal investigation, it was determined that one email account was potentially impacted by this phishing incident. Glaukos immediately performed a password reset for the affected account and swiftly engaged a team of third-party forensic experts to investigate the incident and analyze the affected user account. On February 17, 2021, after a thorough investigation by the third-party forensic experts, Glaukos determined that the affected email inbox contained certain individuals' limited personal information.

Glaukos immediately began working to obtain sufficient contact information for all affected individuals. At this time, Glaukos is aware of two (2) New Hampshire residents who may have been affected by this incident. As our investigation is ongoing, we will provide supplemental notification should we determine additional New Hampshire residents are potentially affected.

Glaukos will promptly notify the affected individuals on March 12, 2021, and offer all affected New Hampshire residents complimentary credit monitoring for twelve (12) months. A copy of the draft notification letter is attached, which outlines the incident and provides affected individuals with additional resources to protect their identity and monitor the credit history and personal accounts. As the letter indicates, Glaukos will be offering credit monitoring and identity restoration services at Glaukos's expense. Glaukos is taking proactive steps to ensure that all state and federal notification obligations are complied with due to this incident.

Please do not hesitate to contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: John Loyal
John Loyal, Esq.

GLAUKOS®
Transforming Glaucoma Therapy

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

RE: NOTICE OF DATA BREACH
Important Security Notification. Please read this entire letter.

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

I am writing to inform you of a data security incident experienced by Glaukos Corporation ("Glaukos") that may have involved your personal information described below.

Glaukos takes the privacy and security of all information very seriously. While we have no evidence to suggest that any of the impacted information was viewed or misused during this incident, it is crucial that we be as supportive and transparent as possible. That is why I am writing to inform you of this incident, to offer information about steps that can be taken to help protect your information, and to let you know about complimentary identity monitoring services that we are offering you through Kroll, a global leader in risk mitigation and response.

What Happened:

On or about October 9, 2020, Glaukos fell victim to an email phishing attack as Glaukos employees were targeted with fraudulent emails containing a malicious link. It was determined that one email account was potentially impacted by the phishing incident. Upon discovery, Glaukos performed a password reset for the affected account and swiftly engaged a team of third-party forensic experts to investigate. On February 17, 2021, after a thorough investigation, Glaukos determined that the affected email inbox contained limited personal information of certain individuals.

Although the forensic investigation could not rule out the possibility that this information may have been accessed by an unknown third-party actor, there is no indication that any information was actually viewed or transferred from the email account. However, we are providing this notification to you out of an abundance of caution and so that you may diligently monitor your personal information and resources. We take great care in the security of our technology systems and regret that this incident has occurred.

What Information Was Involved:

It is important to note, as mentioned above, that there is no evidence to suggest that any personally identifiable information has been accessed, viewed or misused. The personal information that could have been accessed by the unauthorized individual(s) may have included your first and last name, in combination with your <<b2b_text_1(ImpactedData)>>.

What We Are Doing:

Glaukos has taken every step necessary to address the incident and is committed to fully protecting all of the information that you have entrusted to us. Unfortunately, network intrusions have become more common and this incident experienced by Glaukos is similar to other experiences by other companies across a range of industries and practice areas. Upon learning of this incident, we immediately secured the affected accounts, reset passwords, and took steps to enhance the security of all information to help prevent similar incidents from occurring in the future. We retained a third-party forensic firm to conduct a thorough investigation and are offering you complimentary identity monitoring services.

Identity Monitoring Services:

In an abundance of caution and to help relieve concerns,we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services includes twelve (12) months of Credit Monitoring, Fraud Consultation, and Identity Restoration through Kroll.

Additional information regarding how to activate your complimentary identity monitoring services is enclosed.

What You Can Do:

- Activate your Identity Monitoring Services – To activate your free identity monitoring services visit https://enroll.idheadquarters.com use your membership number, <<Member ID>>, and follow the steps to receive your identity monitoring service online within minutes. Please note the deadline to activate is June 18, 2021. We encourage you to contact Kroll with any questions at 1-855-498-2049 between 8:00 am and 5:30 pm Central Time Monday through Friday.
- Review credit reports –We recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not recognize or understand, consult with Kroll or contact the credit agencies directly. You may also wish to place a fraud alert or credit freeze on your credit files. Please review the "Information about Identity Theft Protection", which can be found in the reference guide included with this letter for additional information about these options.
- Review your credit and debit card accounts. It is always good practice to monitor your account activity regularly to reduce your risk of becoming a victim. If you see something you do not recognize, immediately notify the financial institution as well as the proper law enforcement authorities.

Additional Resources:

Included below is a reference guide: "ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCE OF IDENTITY THEFT", which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection.

For More Information:

Should you have questions or concerns regarding this matter, please do not hesitate to contact us at 1-855-498-2049 between 8:00 am and 5:30 pm Central Time Monday through Friday.

Glaukos has no relationship more important or more meaningful than the one we share with you. I want to personally express my deepest regret for any worry or inconvenience that this incident may cause you.

Sincerely,

Diane Biagianti

Diane Biagianti
Sr. Vice President, General Counsel

ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

➢ PLACE A 1-YEAR FRAUD ALERT ON YOUR CREDIT FILE

An **initial 1-year security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request when a fraud alert is active. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

TransUnion	**Experian**	**Equifax**
Fraud Victim Assistance Dept.	National Consumer Assistance	Consumer Fraud Division
P.O. Box 2000	P.O. Box 9554	P.O. Box 740256
Chester, PA 19016-2000	Allen, TX 75013	Atlanta, GA 30374
1-800-680-7289	1-888-397-3742	1-800-525-6285
www.transunion.com	www.experian.com	www.equifax.com

➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report in connection with any new credit application, which will prevent them from extending credit. A security freeze generally does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting agencies. You should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. In order to request a security freeze,you will need to provide some or all of the following informationto the credit reporting agency, depending on whether you do so online, by phone, or by mail: 1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.); 2. Social Security Number; 3. Date of birth; 4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years; 5. Proof of current address,suchas a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2;8. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

You can obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every twelve (12) months. Visit www.annualcreditreport.com or call 1-877-322-8228. 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.

➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with; and shredding receipts, statements, and other sensitive information. Remain vigilant by reviewing account statements and monitoring credit reports.

➢ USE TOOLS FROM CREDIT PROVIDERS

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

➢ BE AWARE OF SUSPICIOUS ACTIVITY INVOLVING YOUR HEALTH INSURANCE

Contact your healthcare provider if bills do not arrive when expected, and review your Explanation of Benefit forms to check for irregularities or suspicious activity. You can also contact your health insurance company to notify them of possible medical identity theft or ask for a new account number.

➢ RIGHTS UNDER THE FAIR CREDIT REPORTING ACT (FCRA)

You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to your employees; (v) you may limit "prescreened" offers of credit an insurance you get based on information in your credit report; (vi) and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.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.

➢ OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. Additionally, any suspected identity theft should be reported to law enforcement, including your state Attorney General and the Federal Trade Commission. Additional information is available at http://www.annualcreditreport.com.

- Visit http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding protecting your identity.
- The Federal Trade Commission has an identity theft hotline: 1-877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.ftc.gov/idtheft. For Mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, DC 20580.
- **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.
- **For New York residents,** you may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotectionl; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.
- **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.
- **For Rhode Island Residents,** the Attorney General can be contacted at 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov or 1-401-274-4400.

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.