

June 28, 2022

Michael H Hinckle
michael.hinckle@klgates.com

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

Attorney General Brian E. Frosh
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

T +1 919 466 1115
F +1 919 831 7040

Dear Attorney General Frosh:

Pursuant to the Maryland Personal Information Protection Act (“PIPA”), we write on behalf of our client, Goldsboro Podiatry, to notify you of a data security incident involving five (5) Maryland residents.

IDENTIFICATION OF PARTIES

The entity that experienced the incident is Goldsboro Podiatry, a medical group practice located at 407 N Herman St, Goldsboro North Carolina, 27530 (the “Practice”). The Practice is a covered entity under the federal Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (“HIPAA”).

Please note that the Practice is not located in Maryland. Rather, the affected Maryland residents were treated at the Practice while traveling to or temporarily residing in the State of North Carolina.

NATURE OF THE DATA SECURITY INCIDENT

Goldsboro Podiatry maintains electronic records for its patients and uses an external provider (the “Service Provider”) to store this patient data. On or about Friday, April 29, 2022, the Service Provider discovered that certain servers had been the subject of a ransomware attack. Upon discovering this incident, the Service Provider immediately engaged third-party cyber forensics experts to assist in responding to the attack, began an investigation to understand the scope of the incident, and contacted law enforcement (the Federal Bureau of Investigation).

More recently, in or about May 2022, the Service Provider determined that the personal information that may have been obtained without authorization included that of approximately five (5) Maryland residents. The Service Provider notified our client of this circumstance on or about Friday, May 20, 2022, and we promptly began an investigation into this incident with the full cooperation of the Service Provider.

The forensics experts have completed their investigation and indicated that the personal information that may have been obtained without authorization included names, contact information, dates of birth, Social Security Numbers, demographic information, medical history, medication information, clinical observations and diagnoses, and/or treatment plans.

While the Service Provider knows files were obtained, as of this time, we do not have any evidence that the information in those files has been made public or misused, or that any identify theft fraud has been committed to date. The Service Provider believes that the data that was taken has been deleted.

NOTICE TO INDIVIDUALS AND OTHER STAKEHOLDERS

Notification will be sent to Maryland residents via written notice by the U.S. mail. Notice has not been delayed due to a law enforcement investigation. A sample copy of the notice is attached hereto. In accordance with PIPA, we have notified your office via email prior to sending individual notices to Maryland residents, which we anticipate will occur on or about Tuesday, June 28, 2022.

As a HIPAA covered entity, Goldsboro Podiatry will comply with all other reporting obligations required by law, including notice to the U.S. Department of Health and Human Services.

STEPS THE PRACTICE AND ITS SERVICE PROVIDER HAVE TAKEN OR PLAN TO TAKE RELATING TO THE INCIDENT

The Practice has requested and have received a corrective action report from the Service Provider assuring us of the steps it has taken to address the incident and to help protect against future breaches. Upon discovery of the breach, the Service Provider's cybersecurity team immediately took a series of actions, including conducting a forensic investigation to confirm which company systems were impacted and to better understand the nature of the event, and contacting law enforcement. The Service Provider also further secured its information technology systems, and enhanced its cybersecurity defenses to help prevent future attacks, including by improving capabilities to detect and manage potential vulnerabilities and security incidents, among other things.

Goldsboro Podiatry and the Service Provider will continue to work closely to minimize the risk of incidents like these from happening again.

FREE CREDIT MONITORING

The Practice is offering 24 months of identity theft and credit monitoring services free of charge to the affected individuals, including Maryland residents. The attached sample letter describes these services in more detail, as well as other steps individuals can take to protect themselves from potential harm. Further description of the services is available here: <https://www.experianidworks.com>.

CONTACT INFORMATION

Your office may contact me at 919-466-1115 or michael.hinckle@klgates.com should you have any questions or need further information.

Respectfully submitted,



Michael H. Hinckle

cc: Kevin Wolf, DPM, Goldsboro Podiatry

Attachment



Return Mail Processing
PO Box 999
Suwanee, GA 30024

119 1 30666 *****AUTO**ALL FOR AADC 283

SAMPLE A. SAMPLE - L01

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



June 29, 2022

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

Dear Sample A. Sample:

We write to inform you, as a patient of Goldsboro Podiatry, of a data security incident that may involve some of your personal information and personal health information. We take the protection of your information very seriously, and we are contacting you directly to explain the circumstances of the incident and the steps we and our service provider are taking in response.

What Happened?

Goldsboro Podiatry maintains electronic records for its patients and uses an external provider (the "Service Provider") to store this patient data. On or about Friday, April 29, 2022, the Service Provider discovered that certain servers had been the subject of a ransomware attack. Upon discovering this incident, the Service Provider immediately engaged third-party cyber forensics experts to assist in responding to the attack, began an investigation to understand the scope of the incident, and contacted law enforcement. More recently, in or about May 2022, the Service Provider discovered that certain information related to you may have been obtained without authorization from the servers during the cyberattack.

The Service Provider notified us of this circumstance on or about Friday, May 20, 2022, and we promptly began an investigation into this incident with the full cooperation of the Service Provider. There is no evidence that the information that may have been obtained without authorization has been made public or that any identity theft or fraud has been committed to date.

Goldsboro Podiatry is working closely with the Service Provider to address this issue, to take steps to secure your personal information, and to provide support to its patients who may have been affected by this incident.

What Information Was Involved?

The information that may have been obtained without authorization included names, contact information, dates of birth, Social Security Numbers, demographic information, medical history, medication information, clinical observations and diagnoses, and/or treatment plans.

What We Are Doing To Protect Your Information:

We requested and have received a corrective action report from the Service Provider assuring us of the steps it has taken to address the incident and protect against future breaches. Upon discovery of the breach, the Service Provider's cybersecurity team immediately took a series of actions, including conducting a forensic investigation to confirm which company systems were impacted and to better

Dr. Kevin J. Wolf

407 N. Herman St. • Goldsboro, NC 27530 • 919-583-9788 • Fax 919-583-9790

understand the nature of the event, and contacting law enforcement. The Service Provider also further secured its information technology systems, and enhanced its cybersecurity defenses to help prevent future attacks, including by improving capabilities to detect and manage potential vulnerabilities and security incidents, among other things.

Protecting your personal information is of utmost concern to us. To help protect your information, the Service Provider has agreed to provide you with identity detection and resolution tools through Experian, one of the leading credit and identity monitoring companies, through a complimentary 24-month membership to Experian's® IdentityWorksSM. To activate this membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: September 30, 2022**. Your **activation code** will not work after this date.
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877.890.9332 by **September 30, 2022**. Be prepared to provide engagement number **B054065** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING THE 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 agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your personal information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.890.9332. 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 (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 support is available as part of the membership being provided at no cost to you and is effective from the date of this letter. Registration is not required to access the service provided by Experian's Identity Restoration Specialists. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* 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.

What You Can Do:

We want to make sure you are aware of the additional steps you may take to guard against the use of your personal health and other information and protect yourself from potential harm resulting from this breach.

As you are likely aware, cyberattacks increasingly threaten the security of information at work and at home. You should remain vigilant by reviewing account statements and monitoring free credit reports. Please see the attachment for further steps you can take to protect your personal information as well as additional important information. We also ask you to remain vigilant against any attack and to monitor your personal accounts for any suspicious computer-related activity.

Below we have included the contact information for the major consumer reporting agencies:

Experian
P.O. Box 4500
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-813-5604

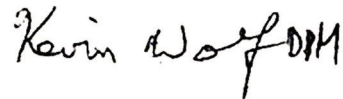
Equifax
P.O. Box 740256
Atlanta, GA 30374
1-888-378-4329

For More Information:

As noted, please see the attachment, particularly if you are a U.S. citizen or resident, for further steps you can take to protect your personal and/or organizational information as well as additional important information.

We sincerely apologize for this incident and regret any inconvenience it may cause. Should you have questions or concerns regarding this matter, please call 800-558-5200.

Sincerely,

A handwritten signature in black ink that reads "Kevin Wolf" with a stylized flourish at the end.

Dr. Kevin J. Wolf
Goldsboro Podiatry

Attachment

ATTACHMENT

What You Can Do:

- Be on the alert for suspicious activity related to your accounts, credit report and financial products. We cannot exclude the possibility that third parties may attempt to use some of your personal information for financial gain.
- If you suspect an incident of identity theft has occurred, find suspicious activity on your credit reports or have reason to believe your information is being misused, file a police report and/or contact a major credit bureau, other local law enforcement, your state attorney general, or the Federal Trade Commission. Get a copy of any report as you may need it to clear up any fraudulent debts.
- Fraud Alert. Call one of the major credit bureaus listed below to place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days. You can obtain further information about fraud alerts and security freezes from the credit bureaus.
- Security Freeze. You may also place a security freeze on your credit reports, free of charge. A security freeze generally requires submitting to the credit bureau your full name, address (including past addresses within the last five years), proof of current address, a legible photocopy of a government issued identification card, social security number, and date of birth. 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. 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. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze with each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com). To place a security freeze on your credit report, you may send a written request by regular, certified or overnight mail at the addresses below. You may also place a security freeze through each of the consumer reporting agencies' websites or over the phone, using the contact information below:
 - **Equifax**, P.O. Box 740256, Atlanta, GA 30374: equifax.com or 1-888-378-4329
 - **Experian**, P.O. Box 4500, Allen, TX 75013: experian.com or 1-888-397-3742
 - **TransUnion**, P.O. Box 2000 Chester, PA 19016: transunion.com or 1-800-813-5604
- Free Credit Report. We also recommend you periodically request that credit reports from all available major credit bureaus be sent to you, free of charge, for your review. Checking your credit reports periodically can help you spot problems and address them quickly. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228.
 - For Colorado, Georgia, Maryland, Massachusetts, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

- Federal Trade Commission. You can obtain additional information about preventing identity theft, fraud alerts and security freezes from the Federal Trade Commission ("FTC"), 600 Pennsylvania Avenue, NW, Washington, DC 20580: 877-382-4357, <https://consumer.ftc.gov/identity-theft-and-online-security>. You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The Consumer Financial Protection Bureau (CFPB) has published a list of the primary rights created by the FCRA at https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.
- Iowa Residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
- Maryland Residents: Further information about security breach response and identity theft prevention and protection can be obtained from Maryland's Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 410-576-6300; or <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>.
- Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. The Attorney General can be contacted at One Ashburton Place, 18th Floor, Boston, MA 02108; 617-727-8400; or <https://www.mass.gov/orgs/office-of-attorney-general-maura-healey>.
- New Mexico Residents: 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, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you would get based on information in your credit report; 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. You can review your 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.
- New York Residents: Further information about security breach response and identity theft prevention and protection can be obtained from New York's Office of the Attorney General, The Capitol, Albany, NY 12224-0341: 1 (800) 771-7755 or <https://ag.ny.gov/internet/privacy-and-identity-theft>.
- North Carolina Residents: Further information about preventing identity theft can be obtained from North Carolina's Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001: (919) 716-6000; or <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>.