2024-168

PHYSICIANS TO WOMEN, INC.

Return mail will be processed by: IBC
PO Box 847 • Holbrook, NY 11741

[redacted]

January 26, 2024

NOTICE OF SECURITY INCIDENT

Dear [redacted]:

Physicians To Women ("PTOW"), a division of Mid-Atlantic Women's Care, PLC ("MAWC"), is providing notice of an event that impacts the privacy of some of your personal information. PTOW and MAWC take this incident very seriously and are providing information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On or around April 4, 2023, MAWC was notified of suspicious activity within PTOW's network. In response, we immediately took steps to secure our systems and initiated an investigation into the nature and scope of the event with the assistance of third-party computer forensic specialists. The investigation determined that an unauthorized actor gained access to certain systems in PTOW's network and acquired certain files from those systems on April 4, 2023. We identified the affected files and engaged a data review vendor to conduct a comprehensive and time-consuming review of the files in order to identify the type of information contained therein, and to whom the information relates. On July 5, 2023, we received the results of this extensive review process from the data review vendor and identified that information pertaining to certain current and former patients and/or their guarantor(s) was present in the affected files, including you. Since then, we have been performing additional work to review and verify the affected information as well as locate address information in order to provide direct notice to as many impacted individuals as possible.

What Information Was Involved? Our review determined that the following types of information were present in the affected files that were accessed and acquired by the unauthorized actor: your name, [redacted] Although the investigation was unable to confirm whether your information was actually viewed by the unauthorized actor, we are unable to rule out this possibility. Please note that we are not aware any actual or attempted fraudulent misuse of information as a result of this incident.

What We Are Doing. The confidentiality, privacy, and security of personal information is among our highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this incident, we immediately took steps to secure our systems and performed a full investigation. We have implemented additional security measures to further protect against similar incidents moving forward. Federal law enforcement is aware of this incident, and we also notified applicable regulators, including the U.S. Department of Health and Human Services.

Additionally, we are offering you credit monitoring and identity theft protection services for 24 months through Experian, at no cost to you. **The deadline to enroll in these services is March 31, 2024.** Please note that you will not be automatically enrolled in these services. Should you wish to do so, you will need to enroll yourself in these services, as we are not able to do so on your behalf. You may find instructions on how to enroll in these services in the enclosed *Steps You Can Take to Help Protect Personal Information.*

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Personal Information.* There you will also find more information on the complimentary credit monitoring and identity theft protection services we are making available to you.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions or need assistance, please call our dedicated assistance line at 888-814-2208 between the hours of 9:00 am - 7:00 pm Eastern Time, Monday through Friday, excluding all major U.S. holidays. You may also write to PTOW at 21 Highland Ave SE, Suite 200, Roanoke, VA 24013.

We sincerely regret any inconvenience or concern this incident may cause you. Protecting your information is very important to us, and we remain committed to safeguarding the information in our care.

Sincerely,

Physicians To Women
A division of Mid-Atlantic Women's Care, PLC

UWHW2-ADT-24

Steps You Can Take to Help Protect Personal Information

Enroll in Credit Monitoring and Restoration

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 24 months.

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 March 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: [redacted]

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 1-877-288-8057 by March 31, 2024. Be prepared to provide **engagement number B113913** 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, Equifax and Transunion files 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com, call, toll-free, 1-877-322-8228, or by completing an Annual Credit Request Form at: *www.ftc.gov/bcp/menus/consumer/credit/rights.shtm* and mailing the form to:

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

You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a security freeze, you may need to provide the following information, depending on whether the request is made online, by phone, or by mail:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax
1-888-298-0045
https://www.equifax.com/personal/credit-report-services/

Equifax Fraud Alert
P.O. Box 105069
Atlanta, GA 30348-5069

Equifax Credit Freeze
P.O. Box 105788
Atlanta, GA 30348-5788

Experian
1-888-397-3742
https://www.experian.com/help/

Experian Fraud Alert
P.O. Box 9554
Allen, TX 75013

Experian Credit Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion
1-800-916-8800
https://www.transunion.com/credit-help

TransUnion Fraud Alert
P.O. Box 2000
Chester, PA 19016

TransUnion Credit Freeze
P.O. Box 160
Woodlyn, PA 19094

Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: Office of Policy and Coordination, Room CC5422 Bureau of Completion Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

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. You should also contact your state taxing authority if you have concerns that your tax filings are subject to fraud.

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

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:

https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/. PTOW is located at 21 Highland Ave SE, Suite 200, Roanoke, VA 24013.

For 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 bureaus 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 get based on information in your credit report; and you may seek damages from 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 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 New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov/.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.