ECKERT SEAMANS
ATTORNEYS AT LAW

RECEIVED
MAY 28 2019
CONSUMER PROTECTION

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

Matthew H. Meade
Direct 412-566-6983
mmeade@eckertseamans.com

May 22, 2019

VIA FIRST CLASS MAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Sir or Madam:

This notice is provided on behalf of my client Doctors' Management Service, Inc. ("DMS"), pursuant to N.H. Rev. Stat. § 359-C:20(I)(b). DMS experienced an incident that impacted its computer systems that may have resulted in unauthorized access to certain information that DMS maintains. On May 17, 2019, DMS notified five (5) New Hampshire residents who were impacted by the breach. These individuals are doctors whose credentialing information, including Social Security number, was maintained by DMS. A copy of the notice that DMS sent to the affected New Hampshire is attached.

On December 24, 2018, DMS first noticed technical issues with its computer network. DMS immediately began an investigation to identify what had happened and how it happened. Through its investigation, DMS discovered that encryption malware was affecting its server. Leading forensic investigators then joined the investigation to determine the full nature and scope of the incident. DMS worked closely with those investigators to conduct a thorough review of available forensic evidence, to determine whether any of the data on the server was subject to unauthorized access or exfiltration as a result of this incident. DMS's investigation determined the following:

- DMS's server became encrypted with the GandCrab variant of ransomware.
- Initial unauthorized access to the DMS network took place on April 1, 2017 through Remote Desktop Protocol (RDP) on a DMS workstation. DMS did not detect any unauthorized access to its server until ransomware was used to maliciously encrypt its files. DMS did not pay the ransom, but instead was able to restore all data through its backups.
- On February 15, 2019, DMS's forensic investigator reported that while the investigation could not determine whether personal information was actually viewed or downloaded, that type of activity could not be ruled out. In an abundance of caution a thorough

review of all information maintained by DMS in the impacted server at the time of the incident was performed to identify any personal information present.

- DMS's forensic investigator contacted law enforcement, and DMS worked with its investigator to complete the investigation.
- DMS has not uncovered any evidence of unauthorized access to, use of, or exfiltration of any data.

Since discovering the breach, DMS has changed its network security system to limit access to its systems from outside of its network, and to improve its network security. DMS in conjunction with outside information security experts is working to help prevent similar occurrences in the future. DMS will continue to educate its staff on cyber best practices. DMS also has offered the New Hampshire residents one (1) year of identity theft protection services, at no cost.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

Matthew H. Meade

MHM/
Enclosure

Doctors' Management Service, Inc.

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Notice of Data Security Incident

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Doctors' Management Service, Inc. ("DMS") values the security of the information you entrust to us. Unfortunately, we are writing to you with important information about an incident that impacted our computer systems. During a recent investigation of a HIPAA data breach, we discovered that in addition to certain patient information, there may have been unauthorized access to your medical credentialing information that was provided to DMS including your name, address and Social Security number. **At this time, we have no indication that any of your information has been inappropriately used by anyone.** However, we are providing this notice to you as a precautionary measure, to inform you of the incident, and to explain steps that you can take to protect your information.

What Happened

On December 24, 2018, DMS first noticed technical issues with our computer network. We immediately began an investigation to identify what had happened and how it happened. Through our investigation we discovered that encryption malware was affecting our server. Leading forensic investigators joined our investigation to determine the full nature and scope of the incident. We worked with them so they could conduct a thorough review of available forensic evidence to determine whether any of the data on the server was subject to unauthorized access or exfiltration as a result of this incident. Our investigation has determined the following:

- Our server became encrypted with the GandCrab variant of ransomware.
- Initial unauthorized access to the DMS network took place on April 1, 2017 through Remote Desktop Protocol (RDP) on a DMS workstation. We did not detect any unauthorized access to our server until ransomware was used to maliciously encrypt our files. We did not pay the ransom, but instead were able to restore all data through our backups.
- On February 15, 2019, our forensic investigator reported that while the investigation could not determine whether personal health information was actually viewed or downloaded, that type of activity could not be ruled out. In an abundance of caution, a thorough review of all information maintained by DMS in the impacted server at the time of the incident was performed to identify any personal information present.
- Our forensic investigator contacted law enforcement and we worked with the investigator to complete our investigation.

What We Are Doing About It

Since discovering the breach, we have changed our network security system to limit access to our systems from outside of our network and to improve our network security. DMS, in conjunction with outside information security experts, is working to help prevent similar occurrences in the future. We will also continue to educate our staff on cyber best practices. Consistent with our compliance obligations and responsibilities, we are providing notice of this incident to you and appropriate state regulators. We also are offering the following services to you at no charge:

1. **Credit Monitoring.** We are offering you a complimentary one-year membership to Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediately identifying and resolving identity theft. IdentityWorksSM Credit 3B is

completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorksSM Credit 3B, including instructions on how to activate your complimentary one-year membership, please see the additional information attached to this letter.

2. **Identity Restoration.** If you believe there was fraudulent use of your information or identity theft, and would like to discuss how to resolve those issues, you may reach out to an Experian agent. If after discussing your situation with an agent it is determined that identity restoration support is needed, an Experian Identity Restoration agent will be 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 creditors 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 this identity restoration offer is available to you for one year 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. You will also find self-help tips and information about identity protection at this site.

What Can You Do

As a precautionary measure, we advise you to take appropriate steps to protect your information. We recommend that you utilize the free credit monitoring service described above and remain vigilant to the possibility of fraud and identity theft by reviewing and monitoring your account statements and free credit reports for any unauthorized activity. If you suspect unauthorized or suspicious activity, you should immediately contact your credit card company, financial institution, and/or law enforcement, or utilize the above-described Identity Restoration service: www.ExperianIDWorks.com/restoration.

You may also request a security freeze be added to your credit report at Experian's online Freeze Center, www.experian.com/freeze/center.html, by phone at 1-888-EXPERIAN (1-888 397-3742), or by mail to Experian Security Freeze, P.O. Box 9554, Allen, TX 75013.

For More Information

If you need more information or have other questions please call our toll free hotline number 1-866-535-9061, Monday through Friday, from 9:00am to 6:30pm EST and we will work with you on next steps.

We sincerely apologize for any inconvenience and concern this incident has caused you. Our team is working to help prevent similar occurrences in the future. The privacy and security of your information is very important to us and we remain committed to doing everything we can to maintain the confidentiality of your information.

Sincerely

Timothy DiBona
Chief Executive Officer
Doctors' Management Services, Inc.

EXPERIAN IDENTITYWORKS℠ CREDIT 3B

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks℠ Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<ClientDef1(Date)>>** (Your code will not work after this date)
2. VISIT the **Experian IdentityWorks** website to enroll: **www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code:** **<<Member ID>>**

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 877-288-8057. Be prepared to provide engagement number <<ClientDef2(Engagement Number)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS℠ CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks℠ Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **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.

Activate your membership today at www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

MORE INFORMATION ABOUT IDENTITY THEFT

AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the Federal Trade Commission by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 303481	Allen, TX 75013	Chester, PA 19022
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice Attorney General's Office
9001 Mail Service Center Raleigh, NC 27699-9001 www.ncdoj.gov
(877) 566-7226