From: Westerhaus, Charles E. < >
Sent: Thursday, August 17, 2023 12:23 PM
To: AG CONSUMER [AG] <consumer@ag.iowa.gov>
Cc: Dort, Kenneth K. < >; Van Fleet, Kelly < >
Subject: Data Breach Notification

Attorney General Bird,

I am writing to inform you about a security incident affecting 713 Iowa residents.

Our firm represents the Morris Hospital & Healthcare Centers ("Morris Hospital"), which experienced a security incident, and we are hereby formally notifying you of this event pursuant to Iowa Code § 715C.2(8) (2023). By providing this notice, Morris Hospital does not waive any rights or defenses regarding the applicability of Iowa law, the applicability of the Iowa Personal Information Security Beach Protection statute, or all/any other applicable laws (including those pertaining to personal jurisdiction).

On April 4, 2023, Morris Hospital discovered it had experienced a security incident. Morris Hospital immediately took steps to contain the incident and retained global cybersecurity professionals to conduct an extensive investigation of the incident. Morris Hospital received the initial findings from the investigation on June 20, 2023. Based on the investigation, forensic evidence indicated that, just before the incident, an unauthorized party had exported data to an external cloud storage platform. The investigation found that these exports contained files with information about current and former employees and their dependents or beneficiaries, as well as current and former patients of Morris Hospital.

The potentially exposed records included the name, address, social security number, medical record numbers and account numbers, diagnostic codes (numeric codes used to identify diagnoses and treatments), and date of birth of current and former employees and their dependents and beneficiaries who have also been patients at Morris Hospital.

Upon discovering the incident, Morris Hospital immediately reset passwords for all employee accounts and suspended employee mobile email access. Morris Hospital identified and removed malicious files and enhanced their monitoring, logging, and detection capabilities.

Please let me know if you have any questions or how we can be of assistance.

Very respectfully,

Charles E. Westerhaus, CIPP/US/E, CIPM
Associate

Faegre Drinker Biddle & Reath LLP
600 E. 96th Street, Suite 600
Indianapolis, Indiana 46240, USA

MORRIS HOSPITAL
& HEALTHCARE CENTERS

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

August 17, 2023

J8746-L02-0000002 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L02
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

RE: Notice of Security Incident

Dear Sample A. Sample,

The Morris Hospital & Healthcare Centers (Morris Hospital) writes to inform you about a recent cybersecurity incident that may have involved your personal information. This letter provides you with information about the nature of the incident and affected data and the immediate and additional corrective measures Morris Hospital has taken to guard against future unauthorized disclosure or misuse of your personal data.

What Happened?
On April 4, 2023, Morris Hospital discovered it had experienced a security incident. Morris Hospital immediately took steps to contain the incident and retained global cybersecurity professionals to conduct an extensive investigation of the incident. Based on that investigation, forensic evidence indicated that, just prior to the incident, there were exports of data to an external cloud storage platform by an unauthorized party. The investigation found that these exports contained files with information about current and former employees and their dependents or beneficiaries, as well as current and former patients of Morris Hospital.

What Information Was Involved?
We are notifying you out of an abundance of caution because information related to you – as both an employee and a patient of Morris Hospital -- may have been identified in the files that the unauthorized party potentially accessed. The potentially exposed records included the name, address, social security number, medical record numbers and account numbers, diagnostic codes (numeric codes used to identify diagnoses and treatments), and date of birth of current and former employees and their dependents and beneficiaries who have also been patients at Morris Hospital.

What We Are Doing
We take the security of your personal information seriously. Therefore, upon discovering the incident, Morris Hospital immediately reset passwords for all employee accounts and suspended employee mobile email access. We identified and removed malicious files and enhanced our monitoring, logging, and detection capabilities.

We retained global security professionals to conduct an independent investigation and assist with our recovery efforts. After several weeks of investigation, they were able to produce a listing of affected directories, which our professionals and outside counsel then used to harvest and review restored files for potentially affected personal information.

While we do not have any information to suggest that your personal information has been used inappropriately or without authorization, we have arranged to make available to you ## months of identity theft resolution services provided by Experian's® IdentityWorks℠ at no charge. Please note that you must enroll to take advantage of this free service, and we encourage you to do so.

What You Can Do
If you have not already done so, you can activate your identity monitoring services by following the instructions in the section below titled *Activating Your Complimentary Identity Monitoring*. As always, please continue to be vigilant about the security of your personal accounts and monitor them for unauthorized activity. Please report any suspicious activity to appropriate law enforcement.

Activating Your Complimentary Identity Monitoring

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for ## 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 ## 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 ##-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** November 30, 2023 (Your 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 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 800-608-8196 by November 30, 2023. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

Additional details regarding your ##-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. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian file 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^{TM}:** 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. 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.

* 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.

For More Information

Again, we take the security of your information seriously and regret any concerns or inconvenience this incident may have caused. Please review the enclosed attachment called Preventing Identity Theft and Fraud for more information about how to protect your personal data. If you have further questions or concerns, or would like an alternative to enrolling online, please call 800-608-8196 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

Sincerely,

Thomas J. Dohm, FACHE
President and CEO

Preventing Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office, or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and access some services free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this letter and at www.identitytheft.gov/#/Know-Your-Rights. For example, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

In addition, at no charge, you can have these credit bureaus place a short-term or an extended "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because a fraud alert tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. Once one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert or have any questions regarding your credit report, please contact any one of the agencies listed below. Please note: no one except you is allowed to place a fraud alert on your credit report.

General contact information for each agency:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016-2000
1-866-349-5191	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

To add a fraud alert:

Equifax	(888) 202-4025, Option 6 or	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian	(714) 830-7000, Option 2 or	https://www.experian.com/fraud/center.html
TransUnion	(800) 916-8800, Option 0 or	https://www.transunion.com/fraud-alerts

You may also place a security freeze on your credit reports, free of charge. A security freeze, also known as a "credit freeze," prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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. Unlike a fraud alert, you must place a security freeze separately on your credit file at each bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

Equifax Security Freeze. 1-888-298-0045. P.O. Box 1057881, Atlanta, GA 30348-0241. www.equifax.com/personal/credit-report-services/credit-freeze;

Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013. www.experian.com/freeze/center.html; or

TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19016-2000. www.transunion.com/credit-freeze

The Federal Trade Commission also provides additional information about credit freezes here: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or another statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement or your state Attorney General.

The Federal Trade Commission can be reached at:

Federal Trade Commission
Consumer Resource Center
600 Pennsylvania Avenue NW Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov **or** www.ftc.gov

OTHER IMPORTANT INFORMATION
You may file a report with your local police or the police in the community where the identity theft occurred. You are entitled to request a copy of your police report filed in that matter.

California residents:
You can visit the California Attorney General's site (www.oag.ca.gov/idtheft) for additional information on protection against identity theft.

Iowa residents:
You are advised to report any suspected identity theft to law enforcement or the Iowa Attorney General.

Kentucky residents:
Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601; phone: 1-502-696-5300; www.ag.ky.gov

Maryland residents:
You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General, 200 St. Paul Place Baltimore, MD 21202; phone: 1-888-743-0023; www.marylandattorneygeneral.gov.

New Mexico residents:
The Fair Credit Reporting Act (FCRA) provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, be told if information in your credit file has been used against you, and seek damages from violators. You may have additional rights under the FCRA not summarized here, and identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. You can review these rights by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York residents:
The Office of the Attorney General may be reached at The Capitol, Albany, NY 12224-0341; phone: 1-800-771-7755; ag.ny.gov

North Carolina residents:
You may obtain information about avoiding identity theft at: North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001; phone: 919-716-6400; ncdoj.gov

Oregon residents:
You may obtain information about avoiding identity theft at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; phone: 1-877-877-9392; www.doj.state.or.us/.

Rhode Island residents:
You may obtain information about preventing and avoiding identity theft from Rhode Island's Attorney General Office: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; phone: 401-274-4400; http://www.riag.ri.gov.

Washington D.C. residents:
You may obtain information about avoiding identity theft at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001; phone: 202-727-3400; https://oag.dc.gov/.

Colorado, Georgia, Maine, 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 bureaus directly to obtain such additional report(s).