大成 DENTONS BINGHAM GREENEBAUM

Kyle W. Miller
kyle.miller@dentons.com
D +1 502 587 3517

Dentons Bingham Greenebaum LLP
3500 PNC Tower
101 South Fifth Street
Louisville, KY 40202
United States

dentons.com

August 18, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Re: Notice of Data Breach

Attorney General Anthony Brown,

We write pursuant to Md. Code Com. Law § 14-3504 et seq. to inform you that UofL Health, Inc. will be sending a notice to Maryland residents advising them of a security incident. On June 20, 2023 UofL Health received a notification regarding access to select UofL Health systems by an unauthorized third-party. The unauthorized third party accessed systems which contained personal information on May 30, 2023. UofL Health took immediate action to mitigate the incident.

The threat actor targeted the MOVEit Transfer zero-day exploit of the vulnerability CVE-2023-34362 and successfully downloaded a total of 536 unique files.

There are approximately three Maryland residents affected.

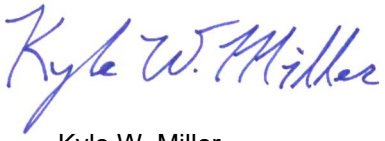
UofL Health has implemented additional security measures upon the guidance and recommendation of their IT professionals to help prevent the reoccurrence of a similar breach and to further protect the privacy of their patients and employees. Upon release of security patches for the CVE-2023-34362 vulnerability, UofL Health stood up an entirely new server in a new environment, installed all available patches, and brought the application online again. Additional administrative and technical remediations include revising data retention policies and extending the retention period of security logs, as well as communicating the new data retention policies to departments and individuals. UofL Health additionally conducted a thorough audit of user accounts and is engaged with departments and users to determine alternative methods for data transfers in order to reduce the attack surface. UofL Health understands the importance of continuous improvement and will remain vigilant in our efforts to identify and mitigate potential security risks.

As a precautionary measure, UofL Health has arranged for impacted individuals to enroll in identity protection services; which includes credit monitoring and identity theft protection. This service will be offered at no cost for at least 24 months.

A formal notice of the incident will be sent by U.S. mail to the individuals for whom UofL Health has identified a mailing address. A copy of the anticipated notice is attached. UofL Health will alert all others via a national press release and information on their web site today. Details for enrollment will be included in the notification letter received by those who are potentially affected or who call in to the call-center referenced in the notification letter or press release.

Please contact me if you have any questions.

Sincerely,



Kyle W. Miller

Enclosure

UofL Health

EPIQ Return Address
EPIQ Return Address
EPIQ Return Address
EPIQ Return Address

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>> <<Date>>

Notice of Data Breach

Dear <<Name 1>><<Name 2>>,

We are writing to tell you about a data breach that exposed some of your personal information and to explain the circumstances of the incident.

What happened?

On June 1, 2023, UofL Health received an alert from its third party security vendor that it may have been one of the thousands of organizations affected by the zero day MOVEit software vulnerability. A small handful of UofL Health medical practices employed the software to securely transmit patient files. UofL Health promptly engaged a forensic investigator to determine the effects, if any, of the vulnerability on UofL Health and its patients. On June 21, 2023 the forensic investigator finished its investigation revealing that the vulnerability allowed an unauthorized party to access certain files.

What information was involved?

UofL Health determined the exact files and contents which were accessed by the attacker. After reviewing the files it has identified the following data elements related to you that were in the accessed files: <<VText>>.

What we are doing.

UofL Health is committed to the confidentiality and security of patient information and continues to evaluate and enhance its security protocols for third party service providers. UofL Health is notifying the patients whose information was identified in the files involved in this breach so that they may protect themselves. We are also offering complimentary credit monitoring and identity theft protection services through Equifax to any affected individual.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

UofL Health has created a dedicated, toll-free call center to answer any questions patients may have. If you have questions, please call 1-833-627-2802, Monday through Friday, between 8:00 a.m. and 5:30 p.m Eastern Time, excluding major U.S. holidays.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

Shelly Denham

Shelly Denham RN, BSN, CHC, CHCO, CHPC, CHRC
Senior Vice President, Compliance, Enterprise Risk & Audit Services
UofL Health, Inc.

– OTHER IMPORTANT INFORMATION –

Enrolling in Complimentary 24-Month Credit Monitoring.

EQUIFAX®

Enter your Activation Code: *<ACTIVATION CODE>*
Enrollment Deadline: *<DEADLINE MMMM DD, YYYY>*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of <***ACTIVATION CODE***> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

[1]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. [2]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. [3]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com [4]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. 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**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont 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).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.