

# Morgan Lewis

**Mark L. Krotoski**

Partner

+1.650.843.7212

mark.krotoski@morganlewis.com

**VIA EMAIL**

January 1, 2022

Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place, 25<sup>th</sup> Floor  
Baltimore, MD 21202  
Email: [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)

Re: Notice of Data Breach

Dear Sir or Madame:

On behalf of North Broward Hospital District d/b/a Broward Health ("Broward Health"), pursuant to Md. Code Com. Law § 14-3501 *et seq.*, we are writing to notify you of a data security incident involving 2,331 Maryland residents.

**Name and Address of Business and the Type of Business**

Broward Health is a public, non-profit hospital system governed by the North Broward Hospital District Board of Commissioners. Broward Health is located at 1800 NW 49th Street, Fort Lauderdale, FL 33309.

**Nature of the Security Incident**

On October 15, 2021, an intruder gained unauthorized access to the Broward Health network and accessed personal medical information of certain patients and personal information of certain employees. The investigation determined the intrusion occurred through the office of a third-party medical provider who is permitted access to the system to provide healthcare services. This criminal activity was promptly reported to the FBI and DOJ.

**What Information Was Involved?**

The personal medical information that was accessed included name, date of birth, address, phone number, financial or bank account information, Social Security number, insurance information and account number, medical information including history, condition, treatment and diagnosis, medical record number, driver's license number and email address. The personal information of employees that was involved included Social Security and financial account number. This personal medical and personal information was exfiltrated, or removed, from Broward Health's systems, however, there is no evidence the information was actually misused by the intruder.

**Morgan, Lewis & Bockius LLP**

1400 Page Mill Road  
Palo Alto, CA 94304  
United States

 +1.650.843.4000  
 +1.650.843.4001

**Response to the Incident**

Broward Health promptly contained the incident upon discovery on October 19, 2021, notified the FBI and the Department of Justice (DOJ), required all employees to update their passwords and engaged an independent cybersecurity firm to conduct an extensive investigation into the incident to determine the nature and scope of the incident. The DOJ requested that Broward Health delay any notification through December 31, 2021, to ensure that the notification did not compromise the ongoing law enforcement investigation.

Broward Health required a password reset with enhanced security measures across the enterprise and the implementation of multifactor authentication for all users of its systems. Broward Health has also begun implementation of additional minimum-security requirements for devices that are not managed by Broward Health Information Technology that access the network, which will become effective in January 2022.

The Maryland residents were notified on January 1, 2022 upon the conclusion of the period of delayed notification requested by the DOJ. A sample notification letter is attached.

**Identity Theft Protection**

Broward Health is providing a complimentary two-year membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides identity detection and resolution of identity theft. None of the notified individuals have been asked or required to waive any right of private action as a condition of accepting the credit monitoring services.

**Contact Information**

If you have any questions concerning this matter, please contact me on behalf of Broward Health at (650) 843-7212, or [mark.krotoski@morganlewis.com](mailto:mark.krotoski@morganlewis.com).

Sincerely,



Mark L. Krotoski

Enclosure

Sample Notification Letter



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

January 1, 2022



Re: Notification of Breach Involving Personal Medical Information



At Broward Health, protecting the personal and medical information of our patients is one of our top priorities. In this regard, I am writing to inform you of a recent isolated incident involving your personal medical information. Although we have no evidence that your personal information has been misused, we are writing to make you aware of the security incident so that you may take any necessary precautions and to offer identity monitoring services at no cost to you to further protect your information.

### **What Happened?**

On October 15, 2021, an intruder who gained unauthorized access to the Broward Health network may have accessed some of your personal information. Broward Health discovered the intrusion on October 19, 2021. Broward Health promptly contained the incident upon discovery, notified the FBI and the Department of Justice (DOJ), required all employees to update their passwords and engaged an independent cybersecurity firm to conduct an extensive investigation into the incident.

The investigation determined the intrusion occurred through the office of a third-party medical provider who is permitted access to the system to provide healthcare services. Broward Health also engaged an experienced data review specialist to conduct an extensive review of the data, which determined that your personal medical information was included in data accessed by the intruder. We are alerting you to this situation now that the involvement of your personal medical information has been confirmed.

The DOJ requested that Broward Health briefly delay this notification to ensure that the notification does not compromise the ongoing law enforcement investigation.

### **What Information Was Involved?**

The personal medical information that was accessed may have included your name, date of birth, address, phone number, financial or bank account information, Social Security number, insurance information and account number, medical information including history, condition, treatment and diagnosis, medical record number, driver's license number and email address. This personal information was exfiltrated, or removed, from Broward Health's systems, however, there is no evidence the information was actually misused by the intruder.

0000003



## What We Are Doing

Broward Health takes the protection of your personal and medical information very seriously. We regularly review our systems as well as our privacy and security practices to enhance those protections. In response to this incident, Broward Health is taking steps to prevent recurrence of similar incidents, which include the ongoing investigation, a password reset with enhanced security measures across the enterprise, and the implementation of multifactor authentication for all users of its systems. We have also begun implementation of additional minimum-security requirements for devices that are not managed by Broward Health Information Technology that access our network, which will become effective in January 2022.

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks<sup>SM</sup>. This product provides you with superior identity detection and resolution of identity theft. The attachment to this letter provides detailed instructions on how you can activate your membership to begin monitoring your personal information.

## What You Can Do

Although we have no evidence that your information has been misused, we want to make you aware of resources you may access to help safeguard your personal information.

Even though we have no indication that your personal information has been used to commit fraud, we recommend that you consider steps to protect yourself from medical identity theft. Medical identity theft occurs when someone uses an individual's name, and sometimes other identifying information, without the individual's knowledge to obtain medical services or products, or to fraudulently bill for medical services that have not been provided. We suggest that you regularly review the explanation of benefits statements that you receive from your health plan. If you see any service that you did not receive, contact the health plan at the number on the statement.

We also recommend that you monitor your financial accounts and if you see any unauthorized activity, promptly contact your financial institution. You may also obtain a free copy of your credit report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also obtain a free copy of your credit report by contacting any one or more of the following national consumer reporting agencies:

**Equifax**  
1-866-640-2273  
[www.equifax.com](http://www.equifax.com)  
P.O. Box 740241  
Atlanta, GA 30374

**Experian**  
1-888-397-3742  
[www.experian.com](http://www.experian.com)  
P.O. Box 2002  
Allen, TX 75013

**TransUnion**  
1-855-681-3196  
[www.transunion.com](http://www.transunion.com)  
P.O. Box 2000  
Chester, PA 19016

You may also choose to contact the three national credit reporting agencies listed above for information about placing a "fraud alert" and/or a "security freeze" on your credit report to further detect any possible misuse of your personal information. You can request a freeze of your credit file free of charge. Contact the Federal Trade Commission for additional information about "fraud alerts" and "security freezes," and about how to monitor and protect your credit and finances.

Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, D.C. 20580  
(202) 326-2222  
[www.ftc.gov](http://www.ftc.gov)

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;

4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. Social Security Card, pay stub, or W2;
8. 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.

The credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (including name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report. You may also temporarily lift a security freeze for a specified period of time rather than for a specific entity or individual, using the same contact information above. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for request made by mail) after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must make a request to each of the credit reporting agencies by mail, through their website, or by phone (using the contact information above). You must provide proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have between one (1) hour (for requests made online) and three (3) business days (for requests made by mail) after receiving your request to remove the security freeze.

- **Police Report:** You have the right to obtain any police report filed in regard to 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 report may be filed in the location in which the offense occurred, or the city or county in which you reside.
- **Additional State Guidance:** Additional information is listed on the second page of the attachment (Additional Details Regarding Your 24-Month Experian's® IdentityWorks<sup>SM</sup> Membership).

### For More Information

We understand that this incident may pose an inconvenience to you, and we sincerely regret that this situation has occurred. Broward Health is committed to protecting the privacy and security of your personal medical information, and we want to assure you that we have implemented appropriate measures to safeguard that information. We value the trust you have placed in us, and we thank you for trusting Broward Health with your healthcare.

If you have questions or concerns about this incident, please call: **(855) 862-8553**, Monday through Friday 9 am – 11 pm EST, Saturday and Sunday 11 am – 8 pm EST (excluding major U.S. holidays), or email: [privacy@browardhealth.org](mailto:privacy@browardhealth.org). Be prepared to provide your engagement number [REDACTED].

Very truly yours,

*Brian W. Kozik*

Brian Kozik  
Senior Vice President, Chief Compliance & Privacy Officer

0000003



**ATTACHMENT**  
**EXPERIAN'S® IDENTITYWORKS<sup>SM</sup>**

As noted in the attached letter, Broward Health is offering a complimentary 2-year membership of Experian's® IdentityWorks<sup>SM</sup> which provides you with superior identity detection and resolution of identity theft.

**To activate your membership and start monitoring your personal information, please:**

- Name: [REDACTED]
- Ensure that you **enroll by: April 30, 2022** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **www.experianidworks.com/credit**
- Provide your **activation code:** [REDACTED]
- 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 (855) 862-8553 by **April 30, 2022**. Be prepared to provide **engagement number** [REDACTED] as proof of eligibility for the identity restoration services by Experian.

**Additional Details Regarding Your Free 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 ExtendCARE<sup>TM</sup>:** 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<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (855) 862-8553. 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 this Identity Restoration support 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](http://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.

## Additional State Guidance

**For residents of *Hawaii, Michigan, New Mexico, North Carolina, Vermont, and Virginia*:** It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

---

**For residents of *Iowa*:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

---

**For residents of *Maryland, New York, North Carolina, and Rhode Island*:** You can also obtain information from the Maryland, North Carolina, and Rhode Island Offices of the Attorneys General about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

---

### **Maryland Attorney General**

Consumer Protection Div.  
200 St. Paul Place  
Baltimore, MD 21202  
(410) 528-8662  
[www.oag.state.md.us](http://www.oag.state.md.us)

### **NY Attorney General's Office**

Bureau of Internet and  
Technology  
The Capitol  
Albany, NY 12224-0341  
(800) -771-7755  
<https://ag.ny.gov/internet/privacy-and-identity-theftv>  
<https://ag.ny.gov/internet/data-breach>

### **North Carolina Attorney General**

Consumer Protection Div.  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
(877) 566-7226  
(919) 716-6000  
<https://ncdoj.gov/protecting-consumers/>

### **Rhode Island Attorney General**

Consumer Protection Div.  
150 South Main Street  
Providence, RI 02903  
(401) 274-4400  
[www.riag.ri.gov](http://www.riag.ri.gov)

---

**For residents of *District of Columbia*:** You may obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia by visiting <https://oag.dc.gov/consumer-protection>, emailing [consumer.protection@dc.gov](mailto:consumer.protection@dc.gov), calling (202) 442-9828, or mailing Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW Washington, DC 20001.

---

**For residents of *Massachusetts*:** For more information about obtaining a security freeze, see <https://www.mass.gov/service-details/freeze-your-credit>.

---

**For residents of *Oregon*:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at <https://doj.state.or.us>, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

---

