

July 1, 2022

Jeff Karberg
Identity Theft Program
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202Via Electronic Mail: ldtheft@oag.state.md.us**Re: Notice of Data Security Incident**

Dear Mr. Karberg:

I write on behalf of my client, the Florida Birth-Related Neurological Injury Compensation Association ("NICA"), to inform you, pursuant to Md. Code Ann. Comm. Law §14-3504(h), of a data security incident affecting the email accounts of two of its employees. An unknown third-party compromised an employee's email credentials, likely due to phishing, and accessed that employee's email account without authorization. Shortly thereafter, a second employee's credentials were compromised, resulting in unauthorized access to that second employee's email account. Within 48 hours of the initial compromise, NICA discovered the unauthorized access and secured both accounts. NICA informed law enforcement and will cooperate in any investigation they may pursue. NICA also worked with third-party cybersecurity experts to respond to the incident and conduct an investigation.

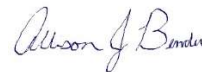
Following a review of the contents of the two affected email mailboxes, NICA identified the personal information of five Maryland residents contained in the mailboxes affected by this incident—two with name, Social Security number and date of birth; three with name, health insurance information, and health or medical health information. While the investigation is ongoing, NICA does not have any evidence that personal information regarding any Maryland resident was in fact accessed. NICA continues to assess options to enhance its security program and prevent similar events from happening in the future.

On July 1, 2022, pursuant to Md. Code Ann. Comm. Law §14-3504(b)(2), NICA will mail notification letters, in the same or substantially similar form as enclosed herein, to affected Maryland residents. The letters include an offer of complimentary credit monitoring and identity theft protection services for a period of twelve months.

Please contact me if you have any questions regarding this matter.

Sincerely,

Dentons US LLP

Allison J. Bender
PartnerAB/mk
Enclosure

Fernanda Lopes & Asociados ► Guevara & Gutierrez ► Paz Horowitz Abogados ► Sirote ► Adepetun Caxton-Martins Agbor & Segun ► Davis Brown ► East African Law Chambers ► Eric Silwamba, Jalasi and Linyama ► Durham Jones & Pinegar ► LEAD Advogados ► Rattagan Macchiavello Arocena ► Jiménez de Aréchaga, Viana & Brause ► Lee International ► Kensington Swan ► Bingham Greenebaum ► Cohen & Grigsby ► Sayarh & Menjra ► For more information on the firms that have come together to form Dentons, go to [dentons.com/legacyfirms](https://www.dentons.com/legacyfirms)



Return Mail Processing
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

July 1, 2022

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

This letter is to inform you that the Florida Birth-Related Neurological Injury Compensation Association (“NICA”) discovered a data security incident affecting email accounts of two of our employees.

Upon discovery of this incident, we worked with third-party cybersecurity experts to respond to the incident and conduct an investigation. We also informed law enforcement and will cooperate in any investigation they may pursue.

Based on our investigation to-date, an unknown third-party compromised an employee’s email credentials and accessed that employee’s email without authorization. Shortly thereafter, a second employee’s credentials were compromised, resulting in unauthorized access to that second employee’s email account. Within 48 hours of the initial compromise, the unauthorized access to both accounts was detected and stopped, and the accounts were secured.

While we do not have any evidence of access to your specific data, we have determined that one or both of these email account mailboxes contained information about you during the period of the compromise. Based on the information available at this time, this incident appears to be financially motivated, and not related to the theft or misuse of your personal data.

What Information Was Involved

These email mailboxes contained personal information regarding patients of NICA and of related individuals that NICA services.

The information about you contained in the mailbox includes the following: <<Variable Data>>.

What We Are Doing

We take the security of your personal data very seriously. We are taking steps to investigate this incident and enhance our security program to help prevent similar incidents from happening in the future, including providing additional training to our workforce around phishing campaigns and security best practices, reviewing and updating our data retention and handling practices, and considering additional tools and software to further harden our environment.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000

insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 1, 2022.

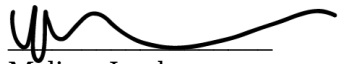
Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment in the enclosed Recommended Steps document. Also, you will need to reference the Activation Code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call IDX at 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,



Melissa Jaacks
Interim Executive Director
Florida Birth-Related Neurological Injury Compensation Association
Post Office Box 14567
Tallahassee, Florida 32317-4567

(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Activation Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX of them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our customer care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an IDX Restoration agent who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place

the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, telephone: 1-888-743-0023.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mall Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone 1-919-716-6400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



Return Mail Processing
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)
Enrollment Code: <<XXXXXXXX>>

To the Parent or Guardian of
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

July 1, 2022

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened

This letter is to inform you that the Florida Birth-Related Neurological Injury Compensation Association (“NICA”) discovered a data security incident affecting email accounts of two of our employees.

Upon discovery of this incident, we worked with third-party cybersecurity experts to respond to the incident and conduct an investigation. We also informed law enforcement and will cooperate in any investigation they may pursue.

Based on our investigation to-date, an unknown third-party compromised an employee’s email credentials and accessed that employee’s email without authorization. Shortly thereafter, a second employee’s credentials were compromised, resulting in unauthorized access to that second employee’s email account. Within 48 hours of the initial compromise, the unauthorized access to both accounts was detected and stopped, and the accounts were secured.

While we do not have any evidence of access to your child’s specific data, we have determined that one or both of these email account mailboxes contained information about your child during the period of the compromise. Based on the information available at this time, this incident appears to be financially motivated, and not related to the theft or misuse of your child’s personal data.

What Information Was Involved

These email mailboxes contained personal information regarding patients of NICA and of related individuals that NICA services.

The information about your child contained in the mailbox includes the following: <<Variable Data>>.

What We Are Doing

We take the security of your child’s personal data very seriously. We are taking steps to investigate this incident and enhance our security program to help prevent similar incidents from happening in the future, including providing additional training to our workforce around phishing campaigns and security best practices, reviewing and updating our data retention and handling practices, and considering additional tools and software to further harden our environment.

In addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include 12 months of CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your child's identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-800-939-4170 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 1, 2022.

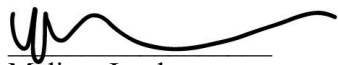
Again, at this time, there is no evidence that your child's information has been misused. However, we encourage you to take full advantage of this service. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment in the enclosed Recommended Steps document. Also, you will need to reference the Activation Code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call IDX at 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,



Melissa Jaacks
Interim Executive Director
Florida Birth-Related Neurological Injury Compensation Association
Post Office Box 14567
Tallahassee, Florida 32317-4567

(Enclosure)

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your child's Enrollment Code provided at the top of the letter.

2. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your child's credit identity.

3. Watch for Suspicious Activity. If you discover any suspicious items and have enrolled in IDX identity protection, notify IDX of them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that your child falls victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your and your child's behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report on behalf of your child if your child experiences identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that your child has been a victim. If you are not the child's parent, you may have to provide documentation to show that you are the child's legal guardian. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

4. Security Freeze. You may place a free credit freeze for children under age 16. By placing a security freeze, someone who fraudulently acquires your child's personal identifying information will not be able to use that information to open new accounts or borrow money in their name. You will need to contact each of the three national credit reporting bureaus listed below to place the freeze, which will prevent anyone from being able to borrow money, obtain instant credit, or get a new credit card on the child's credit, until you or the child upon reaching the age of 18 temporarily lifts or permanently removes the freeze. There is no cost to freeze or unfreeze your child's credit files.

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

5. You can obtain additional information about the steps you can take to help your child avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

Federal Trade Commission: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft for general information about identity theft and <https://consumer.ftc.gov/articles/how-protect-your-child-identity-theft> for information about children's identity theft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.