Board of Developmental Disabilities Services

Northview Center
8114 North Main Street
Dayton, OH 45415
(937) 890-0730
www.mcbdds.org

May 18, 2024

Dear MCBDDS Family,

We are writing to inform you of a situation where some of your personal information could have been affected.

In late February 2024, our Information Technology (IT) staff identified suspicious activity on our computer network. We took immediate and appropriate safeguard actions, retained outside cybersecurity experts to learn as much as we could about the situation, and reported the incident to the Federal Bureau of Investigation (FBI).

The cybersecurity experts began working with our IT team to gather as much information as possible about the incident. After extensive investigation, the cyber team determined this was a ransomware attack, undertaken by an international criminal organization.

The cyber team spent time analyzing our systems and determining what information had been accessed. We learned that personal health information and other sensitive information, such as names, date of birth, birth certificates, Social Security numbers (including copies of the cards), addresses, phone numbers, email addresses, medical records including diagnoses, medical record numbers, banking/checking information, insurance information, and photos could have been affected.

MCBDDS has been working to identify all of the impacted parties and ensure that services would continue uninterrupted throughout this period. Following the guidelines in the federal Health Insurance Portability and Accountability Act (HIPAA), we are in the process of notifying those whose information was affected. In addition to this letter, you will receive a letter addressed specifically to you that lists what type of personal information was disclosed.

What MCBDDS Is Doing to Help Those Affected

If your information was part of the breach, MCBDDS will provide you with identity theft protection and/or credit monitoring services for one year free of charge. If the person affected was younger than 18, we will provide a cyber monitoring product. These services are provided by Cyberscout. **To use these services, you will need to sign up**. There will be instructions in the other letter that explain how to do this.

If you are a person served by MCBDDS and need help signing up for these services, please contact us at 937-739-5335 or at questions@montgomerydds.org.

You will also receive proactive fraud assistance to help with any questions you might have. This service will also be available to you if a criminal uses your information.

What You Can Do to Protect Yourself

We also recommend that you take the following additional precautions:

- **Place** a fraud alert on your credit file so you are notified if anyone tries to open new accounts using your information. To do this, you need to contact all of the following credit bureaus:
    - Equifax: Equifax.com or 888-378-4329
    - Experian: Experian.com or 888-397-3742
    - TransUnion: transunion.com or 888-909-8872

- **Contact** your bank and any other financial institutions and let them know that your information was part of a data breach.

- **Contact** Chex Systems, Inc., which is a nationwide specialty consumer reporting agency under the federal Fair Credit Reporting Act. They can prevent new, unauthorized checking, savings, credit accounts, loans, or other services from being approved in your name without your consent: https://www.chexsystems.com/

- **Monitor** your credit cards and bank accounts for unusual activity.

- **File** an identity theft complaint at the Federal Trade Commission site https://www.identitytheft.gov/ if your personal information has been misused.

- **File** a police report with your local authorities if you find suspicious activity on your credit report. Be sure to get a copy of the police report.

For More Information

Our Superintendent and CEO, Dr. Pamela Combs, will hold several Family and Provider Meetings via Zoom over the next few months to answer questions and share updates. The dates for these are as follows:

- **Tuesday, June 4, 10 a.m.:** https://mcbdds.zoom.us/meeting/register/tZMrdOurqjIrGNNltkqC_Q_N6WdIC9_DIayh
- **Wednesday, June 5, 5:30 p.m.:** https://mcbdds.zoom.us/meeting/register/tZYocuqopjsvE9fzOLvl-HDQT94qcL3CbnTk
- **Thursday, June 6, 2 p.m.:** https://mcbdds.zoom.us/meeting/register/tZclceCrrDIrHdZB4dD-zTU8gpT76Qnt4f8c

We will continue to provide updates on this situation at our Parents and Advocates Advisory Council (PAAC) meetings, which are held via Zoom. Our next meetings will take place **Thursday, May 23** and **Thursday, June 20** at **5:30 p.m.** If you are interested in attending these or future PAAC meetings, please contact our Communications Team at communityrelations@montgomerydds.org and they will send you a link to register for these sessions.

Summary

I have recorded a video explaining this situation, which you can view at https://youtu.be/Rb4n5bNk_L8

We apologize for the inconvenience and concern this incident will cause. We take our responsibility to protect your personal information very seriously.

We urge you to closely monitor your credit and finances, and take advantage of the protection services we're offering. We also ask that you review the enclosed Questions & Answers document for additional details.

Should you have any additional questions for MCBDDS, please contact us at 937-739-5335 or questions@montgomerydds.org.

Sincerely,

Dr. Pamela Combs
Superintendent and CEO

Board of Developmental Disabilities Services

FREQUENTLY ASKED QUESTIONS: Ransomware Attack affecting MCBDDS

1. What happened?

In late February 2024, our IT staff identified suspicious activity on our computer network. We took immediate and appropriate safeguard actions, retained outside cybersecurity experts to learn as much as we could about the situation, and reported the incident to the Federal Bureau of Investigation (FBI). After extensive investigation, the cyber team determined this was a ransomware attack, undertaken by an international criminal organization.

2. What kind of information was affected?

The cyber team spent time analyzing our systems and determining what information had been accessed. We learned that personal health information and other sensitive information, such as names, date of birth, birth certificates, Social Security numbers (including copies of the cards), addresses, phone numbers, email addresses, medical records including diagnoses, medical record numbers, banking/checking information, insurance information, and photos could have been affected.

3. If this incident occurred in February, why are we just hearing about it now?

Our cybersecurity team needed time to determine the nature of the activity and the extent of the attack. This involved gathering as much information as possible about the incident, analyzing our systems, and determining what information was at risk. They also needed to identify the criminals that attacked us and attempt to resolve the situation with them.

MCBDDS has been working to identify all of the potential parties that may have been impacted, and to set up protective services for those people whose information may be at risk. Our team has also been working to ensure that services would continue uninterrupted throughout this period.

4. What are you doing to help people who may be at risk?

If your information was part of the breach, **MCBDDS will provide you with identity theft protection and/or credit monitoring services for one year free of charge.** If the person affected was younger than 18, we will provide a cyber monitoring product. These services are provided by Cyberscout.

To use these services, you will need to sign up. You will receive instructions explaining how to do this in a letter addressed specifically to you. This letter will also tell you what personal information was disclosed.

If you are a person served by MCBDDS and need help signing up for these services, please contact us at 937-739-5335 or at questions@montgomerydds.org.

You will also receive proactive fraud assistance to help with any questions you might have. This service will also be available to you if a criminal uses your information.

--more--

5. What other steps can we take to protect ourselves?

We also recommend that those affected take the following steps:

- **Call** Equifax, Experian and TransUnion to put a fraud alert on your credit file. This will ensure that they will be notified if anyone tries to open new accounts using their information.
- **Contact** your bank and any other financial institutions and let them know your information has been stolen.
- **Contact** Chex Systems, Inc., which is a nationwide specialty consumer reporting agency under the federal Fair Credit Reporting Act. They can prevent new, unauthorized checking, savings, credit accounts, loans, or other services from being approved in your name without your consent: https://www.chexsystems.com/
- **Monitor** your credit cards and bank accounts for unusual activity.
- **File** an identity theft complaint at identitytheft.gov and get other information about how to recover from identity theft.

6. What if I see something suspicious in my credit file, credit card bills, or bank accounts?

- File a police report if you suspect any suspicious activity on your credit report. Be sure to get a copy of the police report in case there is any fraudulent activity on your cards.
- File an identity theft complaint at the Federal Trade Commission site https://www.identitytheft.gov/ if your personal information has been misused.

7. How could something like this happen?

Unfortunately, many criminals target businesses and organizations' computer networks to harvest data illegally every day. Our agency was one of many targeted by these particular criminals right around this time.

We are very sorry this happened, and we apologize for the inconvenience and concern this will cause. We take our responsibility to protect your personal information very seriously.

8. What if I have other questions?

Our Superintendent and CEO, Dr. Pamela Combs, will hold several Family and Provider Meetings via Zoom over the next few months to answer questions and share updates. The dates for these are as follows:

- **Tuesday, June 4, 10 a.m.:** https://mcbdds.zoom.us/meeting/register/tZMrdOurqjIrGNNltkqC_Q_N6WdIC9_DIayh
- **Wednesday, June 5, 5:30 p.m.:** https://mcbdds.zoom.us/meeting/register/tZYocuqopjsvE9fzOLvl-HDQT94qcL3CbnTk
- **Thursday, June 6, 2 p.m.:** https://mcbdds.zoom.us/meeting/register/tZclceCrrDIrHdZB4dD-zTU8gpT76Qnt4f8c

We will continue to provide updates on this situation at our Parents and Advocates Advisory Council (PAAC) meetings, which are held via Zoom. Our next meetings will take place **Thursday, May 23** and **Thursday, June 20** at **5:30 p.m.** Should you be interested in attending these or future PAAC meetings, please contact our Communications Team at communityrelations@montgomerydds.org.

You can also contact us at 937-739-5335 or at questions@montgomerydds.org.

###