

**Colin M. Battersby**  
Direct Dial: (248) 593-2952  
E-mail: [cbattersby@mcdonaldhopkins.com](mailto:cbattersby@mcdonaldhopkins.com)

April 28, 2023

**VIA EMAIL ([consumer@ag.iowa.gov](mailto:consumer@ag.iowa.gov))**

The Honorable Brenna Bird  
Office of the Attorney General  
Consumer Protection Division  
Security Breach Notifications  
1305 E. Walnut Street  
Des Moines, IA 50319-0106

**Re: Iowa PBS Foundation – Incident Notification**

Dear Attorney General Bird:

McDonald Hopkins PLC represents Iowa PBS Foundation. I am writing to provide notification of an incident at Iowa PBS Foundation that may affect the security of personal information of Iowa residents. Iowa PBS Foundation's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any.

On November 20, 2022, Iowa PBS Foundation learned that an unauthorized party obtained access to the Iowa PBS network as a result of a cybersecurity incident. The Iowa PBS Foundation is separate from Iowa PBS, but uses Iowa PBS computer servers and systems to conduct work. Upon learning of this issue, Iowa PBS secured the network and commenced a prompt and thorough investigation in consultation with outside cybersecurity professionals who regularly investigate and analyze these types of situations.

Out of an abundance of caution, Iowa PBS Foundation wanted to inform you of the incident. In the first few days of the investigation, Iowa PBS Foundation learned that a file that contained the names and financial account numbers for approximately 10,000 Iowa PBS Foundation donors was accessible at the time of the incident. It was too early in the investigation to determine whether the file had been accessed or acquired by the threat actor that perpetrated this attack. Nevertheless, Iowa PBS Foundation provided the affected Iowa residents with preliminary notification of the incident on November 23, 2022. As noted, the investigation is ongoing. Iowa PBS Foundation is working to determine whether and to what extent that specific file was actually accessed/acquired, and whether any additional data may have been compromised as part of this incident. To date, Iowa PBS Foundation is not aware of any reports of identity fraud or improper use of any information as a direct result of this incident.

At Iowa PBS Foundation, protecting the privacy of personal information is a top priority. Iowa PBS Foundation is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Iowa PBS Foundation continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

If you have any additional questions, please contact me at (248) 593-2952 or [cbattersby@mcdonaldhopkins.com](mailto:cbattersby@mcdonaldhopkins.com).

Very truly yours,



Colin M. Battersby

Encl.



To Enroll, Please Call:  
[Redacted]  
Or Visit:  
[Redacted]  
[Redacted]  
[Redacted]

[Redacted]

[Redacted]  
[Redacted]  
[Redacted]

**IMPORTANT INFORMATION  
PLEASE REVIEW CAREFULLY**

Dear [Redacted]

The privacy and security of the personal information we maintain is of the utmost importance to the Iowa PBS Foundation (“Iowa PBS”). We are writing with important information regarding a recent security incident that may have impacted some of your information. We want to provide you with information about the incident, tell you about the services that we are providing to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

On November 20, 2022, Iowa PBS experienced a cybersecurity incident and that an unauthorized party obtained access to the Iowa PBS network server. The Iowa PBS Foundation is a separate organization from Iowa PBS, but uses Iowa PBS computer servers and systems to conduct work.

What We Are Doing.

Over the last several months since learning of the incident, we’ve commenced a thorough investigation. As part of our investigation, we have worked very closely with external cybersecurity professionals. After an extensive forensic investigation and manual document review, we discovered that the server accessed contained some of your personal information.

What Information Was Involved?

The server accessed contained some of your personal information, including your full name and Social Security number. While we do not know if your specific information was accessed, out of an abundance of caution we’re informing you of this incident.

What You Can Do.

**To date, we are not aware of any reports of identity fraud or improper use of your information as a direct result of this incident.** Nevertheless, we are offering a complimentary one-year membership of identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include 12 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.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1 [Redacted] or going to [Redacted] and using the Enrollment Code provided above. Iowa PBS Foundation representatives are available Monday through Friday, [Redacted] Please note the deadline to enroll is February 1, 2024.


This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

*For More Information.*

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

**Again, if you have any further questions regarding this incident, please call the Iowa PBS Foundation at (800) 728-2828.**

Sincerely,

  
President  
The Iowa PBS Foundation

– OTHER IMPORTANT INFORMATION –

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

- **Website and Enrollment.** Go to <https://response.idx.us/customending> / <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- **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.
- **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.
- **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](http://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 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 you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist 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.

2. **Placing a Fraud Alert on Your Credit File.**

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

***Equifax***

P.O. Box 105069  
Atlanta, GA 30348-5069  
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>  
(800) 525-6285

***Experian***

P.O. Box 9554  
Allen, TX 75013  
<https://www.experian.com/fraud/center.html>  
(888) 397-3742

***TransUnion***

Fraud Victim Assistance Department  
P.O. Box 2000  
Chester, PA 19016-2000  
<https://www.transunion.com/fraud-alerts>  
(800) 680-7289

3. **Placing a Security Freeze on Your Credit File.**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

***Equifax Security Freeze***

P.O. Box 105788  
Atlanta, GA 30348-5788  
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>  
(888)-298-0045

***Experian Security Freeze***

P.O. Box 9554  
Allen, TX 75013  
<http://experian.com/freeze>  
(888) 397-3742

***TransUnion Security Freeze***

P.O. Box 160  
Woodlyn, PA 19094  
<https://www.transunion.com/credit-freeze>  
(888) 909-8872

In order to place the security freeze, you’ll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

#### **4. Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **[www.annualcreditreport.com](http://www.annualcreditreport.com)**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

#### **5. Additional Helpful Resources.**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

#### **6. Protecting Your Medical Information.**

We have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

**Iowa Residents:** You may contact law enforcement or the Iowa Attorney General’s Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, [www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov), Telephone: 515-281-5164.