PowerSchool Data Security Incident

The privacy and security of the personal information we maintain is of the utmost importance to the Catholic Diocese of Arlington. The Catholic Diocese of Arlington has been monitoring a recent cybersecurity incident that impacted PowerSchool, a company that provides the Catholic Diocese of Arlington with student information management software.

On December 28, 2024, PowerSchool became aware of a cybersecurity incident involving unauthorized exfiltration of certain personal information from PowerSchool Student Information System (SIS) environments through one of PowerSchool's community-focused customer support portals, PowerSource.

Upon learning of the incident, the Catholic Diocese of Arlington promptly inquired with PowerSchool to learn what occurred and to identify what information pertaining to the Catholic Diocese of Arlington was impacted. Despite our attempts to understand the scope of impact, PowerSchool was unable to confirm the exact information that was impacted at the time of the incident. Based on PowerSchool's representations and communications about the incident, the Catholic Diocese of Arlington understands that the impacted information related to the Catholic Diocese of Arlington community may have contained personal information of certain individuals, including one or more of the following: name, limited medical alert information and social security number.

We understand that on or about January 29, 2025, PowerSchool began sending notifications via email directly to certain impacted individuals and families to notify them of the incident. It is anticipated that these incident notification emails from PowerSchool will be sent to affected individuals and families on a rolling basis over a period of weeks.

PowerSchool is offering two years of complimentary identity protection services to students and educators whose information was involved. For adult students and educators, this offer will also include two years of complimentary credit monitoring services. If you are interested in enrolling, please see PowerSchool's provided instructions below:

Option 1 from PowerSchool: If the Involved Individual is 18 or Over

- Ensure that you **enroll by July 31, 2025** (Your code will not work after this date at 5:59 UTC)
- **Visit** the Experian IdentityWorks website to enroll: **www.experianidworks.com/plus**
- Provide your **activation code**: **CTYU949PRK**
- For over the phone assistance with enrollment or questions about the product, please contact Experian's customer care team at 833-918-9464
- Be prepared to provide **engagement number: B138812**

Details Regarding the Experian IdentityWorks Credit Plus 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. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers. 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.

Option 2 from PowerSchool: If the Involved Individual is Under 18

- Ensure that you **enroll by July 31, 2025** (Your code will not work after this date at 5:59 UTC)

- **Visit** the Experian IdentityWorks website to enroll: **www.experianidworks.com/minorplus**
- Provide your **activation code**: **CEBP456TRK**
- For over the phone assistance with enrollment or questions about the product, please contact Experian's customer care team at 833-918-9464.
- Be prepared to provide **engagement number: B138813**

Details Regarding the Experian IdentityWorks Credit Plus 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 enrolled:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. 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.

We encourage impacted individuals to take actions to help protect their personal information. These actions include enrolling in the credit monitoring services described, placing a fraud alert and/or security freeze on their credit files, and/or obtaining a free credit report. Additionally, individuals should always remain vigilant in reviewing their financial account statements, explanation of benefits statements and credit reports for fraudulent or irregular activity on a regular basis and report any suspicious activity to the proper authorities.

PowerSchool has set up a dedicated response line for this incident. Concerned individuals may contact PowerSchool's response line directly at **(833) 918-9464,** available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time. PowerSchool has published additional information on its website, which is available at: **https://www.powerschool.com/security/sis-incident/notice-of-united-states-data-breach/.**

We acknowledge this may be concerning news. As always, our number one priority is to ensure the safety and security of our students, staff and community. We have taken this matter very seriously and will continue to take significant measures to protect the personal information in our possession.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

We recommend that you place a one-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
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329; (800) 525-6285

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

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 916-8800; 800-680-7289

2. Consider 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 cost. 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 sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045; (800) 685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/center.html
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(800) 916-8800; (888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. 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 you do place a security freeze prior to enrolling in a credit monitoring service, 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.

3. 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**. 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.

4. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, 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.

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, 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.

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, Telephone: 888-743-0023.