



**Jackson Lewis P.C.**  
10701 Parkridge Blvd.  
Suite 300  
DC Region, VA 20191  
(703) 483-8300 Main  
(703) 483-8301 Fax  
[www.jacksonlewis.com](http://www.jacksonlewis.com)

*Jackson Biesecker*  
*Direct: (216) 750-4303*  
*Jackson.Biesecker@jacksonlewis.com*

**VIA EMAIL ([idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us))**

Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202

Re: Data Incident Notification<sup>1</sup>

July 31, 2024

Dear Sir or Madam:

Pursuant to Md. Code Com. Law § 14-3504, we are writing on behalf of our client, School District of Beloit (“SDB”), to notify your office of a data security incident affecting two (2) Maryland residents. SDB is located at 1500 Fourth Street, Beloit, WI 53511.

On or about February 9, 2024, SDB discovered it was subject to a criminal ransomware attack (the “Incident”). With assistance from third-party experts, SDB took immediate steps to secure its systems and investigate the nature and scope of the Incident. SDB also reported the Incident to law enforcement.

On or about May 21, 2024, SDB discovered that the Incident may have impacted personally identifiable information (“PII”) for some individuals. The Incident may have involved the following data elements: name, address, Social Security number, driver’s license number or state ID, and/or passport number.

As part of its extensive investigation, SDB worked diligently to identify any PII that may have been subject to unauthorized access or acquisition as a result of the Incident and identify individuals to whom that PII related. This necessitated the time- and labor-intensive process of data mining. The data mining and manual review was ultimately necessary to properly identify potentially affected individuals.

---

<sup>1</sup> Please note that by providing this letter School District of Beloit is not agreeing to the jurisdiction of the State of Maryland, nor waiving its right to challenge jurisdiction in any subsequent actions.

Out of an abundance of caution, and in accordance with applicable law, SDB will provide notice to the affected Maryland residents so that they can take steps to minimize the risk that their information will be misused. SDB will begin sending these notices in the coming days. A sample notice letter is enclosed. Additionally, SDB has arranged for notice recipients to enroll in free credit monitoring and related services for 12 months, including identity theft insurance up to \$1,000,000 as well as identity recovery and restoration services.

As set forth in the enclosed letter, SDB has taken steps to protect the security of the personal information of all individuals. SDB endeavors to protect the privacy and security of sensitive information and has worked diligently to determine how this incident happened and are taking appropriate measures to prevent a similar situation in the future. Since the Incident, SDB has: reset all passwords, implemented a new endpoint detection and response platform, updated its firewall, added additional cybersecurity trainings for staff, and implemented a new network access control platform.

If you require any additional information on this matter, please call me.

Sincerely,

**JACKSON LEWIS, P.C.**

/s/ Jackson E. Biesecker  
Jackson E. Biesecker

Enclosure



School District of

BELOIT

P.O. Box 989728

West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 31, 2024

### **Incident Notice**

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

#### **What Happened**

We are writing to provide information regarding a criminal cyberattack the School District of Beloit ("SDB") was victimized by earlier this year (the "Incident"). We immediately commenced an investigation of the Incident, with assistance from third party experts, for the purpose of determining its scope, the impact on our information systems, and the identities of those the Incident may have affected. We also promptly reported the Incident to the appropriate law enforcement agencies. You are receiving this letter because your personal information may have been impacted.

Through our extensive investigation, we identified a limited set of files that were subject to unauthorized access. We then undertook the time- and resource-intensive steps of data mining and manually reviewing the contents of those files to determine whether they contained personally identifiable information ("PII") and to identify the data subjects to whom that PII related.

On or about May 21, 2024, we determined that, from about January 30 to February 9, 2024, the bad actor may have accessed systems with files that contain PII related to you and a limited number of other individuals. We have not found any evidence that any of your information was misused.

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

The potentially impacted files may have contained your name along with your <<Variable Text 1>>.

#### **What We Are Doing**

Out of an abundance of caution, we are providing this notice to you so that you can take steps to minimize the risk that your information will be misused. The attached sheet describes steps you can take to protect your identity, credit, and personal information.

As an added precaution, we are offering identify theft protection services through IDX. IDX identity protection services include 12 months of credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this specialized protection, IDX can help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-888-488-6132 or going to <https://app.idx.us/account-creation/protect> and using the enrollment code <<ENROLLMENT>>. IDX representatives are available Monday through Friday from 9:00 am to 9:00 pm Eastern Time. Please note that the deadline to enroll is October 25, 2024.

School District of Beloit treats all sensitive information in a confidential manner and is proactive in the careful handling of such information. Since the Incident, we have taken a number of steps to further secure our systems. Specifically, we have: reset all passwords, implemented a new endpoint detection and response platform, updated our firewall, added additional cybersecurity trainings for staff, and implemented a new network access control platform.

### **What You Can Do**

In addition to enrolling in the credit monitoring services discussed above, the attached sheet describes steps you can take to protect your identity, credit, and personal information.

### **For More Information**

Please call 1-888-488-6132 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

We sincerely apologize for this situation and any concern or inconvenience it may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "Willie Garrison II", with a horizontal line extending from the end of the signature.

Dr. Willie Garrison II  
Superintendent  
School District of Beloit

**PLEASE TURN PAGE FOR ADDITIONAL INFORMATION**

## **What You Should Do To Protect Your Personal Information**

We recommend you remain vigilant and consider taking the following steps to protect your personal information:

1. Contact the nationwide credit-reporting agencies as soon as possible to:

Add a fraud alert statement to your credit file at all three national credit-reporting agencies: Equifax, Experian, and TransUnion. You only need to contact one of the three agencies listed below; your request will be shared with the other two agencies. This fraud alert will remain on your credit file for 90 days.

You can also receive information from these agencies about avoiding identity theft, such as by placing a “security freeze” on your credit accounts.

Remove your name from mailing lists of pre-approved offers of credit for approximately six months.

Receive and carefully review a free copy of your credit report by going to [www.annualcreditreport.com](http://www.annualcreditreport.com).

Equifax  
Consumer Fraud Division  
P.O. Box 740256  
Atlanta, GA 30374  
800-525-6285  
[securitymonitoring@equifax.com](mailto:securitymonitoring@equifax.com)

Experian  
Experian Security Assistance  
P.O. Box 72  
Allen, TX 75013  
888-397-3742  
[businessrecordsvictimassistance@experian.com](mailto:businessrecordsvictimassistance@experian.com)

TransUnion  
Consumer Relations & Fraud  
Victim Assistance  
P.O. Box 2000  
Chester, PA 19016  
800-372-8391  
[databreach@Transunion.com](mailto:databreach@Transunion.com)

2. Carefully review all bills and credit card statements you receive to see if there are items you did not contract for or purchase. Also review all of your bank account statements frequently for checks, purchases, or deductions not made by you. Note that even if you do not find suspicious activity initially, you should continue to check this information periodically since identity thieves sometimes hold on to stolen personal information before using it.
3. The Federal Trade Commission (“FTC”) offers consumer assistance and educational materials relating to identity theft, privacy issues, and how to avoid identity theft, such as by setting up fraud alerts or placing a “security freeze” on your credit accounts. The FTC can be contacted either by visiting [www.ftc.gov](http://www.ftc.gov), [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), or by calling (877) 438-4338. If you suspect or know that you are the victim of identity theft, you should contact local law enforcement, and you can also contact the Fraud Department of the FTC, which will collect all information and make it available to law enforcement agencies. The FTC can be contacted at the website or phone number above, or at the mailing address below:

Federal Trade Commission  
Consumer Response Center  
600 Pennsylvania Avenue  
NW Washington, DC 20580

4. *For Maryland Residents:* You can obtain information about steps you can take to help prevent identity theft from the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, [www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov).
5. *For New Mexico Residents:* You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act> or [www.ftc.gov](http://www.ftc.gov). In addition, New Mexico consumers may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information about New Mexico consumers obtaining a security freeze, go to <http://consumersunion.org/pdf/security/securityNM.pdf>.

6. *For New York Residents:* You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: 1) New York Attorney General, (212) 416-8433 or <https://ag.ny.gov>; or 2) NYS Department of State's Division of Consumer Protection, (800) 697-1220 or <https://dos.ny.gov/consumer-protection>.
7. *For North Carolina Residents:* You can obtain information about steps you can take to help prevent identity theft from the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov).