

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Jason Goodwin
JGoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

Phone: (610) 567-0700
Fax: (610) 567-0712

www.C-WLAW.com

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

Jonathan Quagliarello
JQuagliarello@c-wlaw.com

February 6, 2025

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Crystal Lake Elementary District 47 ("District 47") located at 300 Commerce Drive, Crystal Lake, Illinois 60014. We write to provide notification of a recent data security incident. By providing this notice, District 47 does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On October 17, 2024, District 47 experienced a network disruption that affected certain district systems. Upon discovery, District 47 immediately took steps to secure the network and engaged a third-party firm to investigate the incident. Following a full and thorough investigation, District 47 learned that certain information may have been accessed by an unauthorized third party in connection with this incident and engaged in a comprehensive review to determine what information may have been affected and to whom it relates. On January 2, 2025, this review was completed and District 47 worked to identify sufficient contact information to proceed with notification.

On January 31, 2025, District 47 received its results from a National Change of Address (NCOA) search and confirmed this incident potentially affected nine (9) Maryland residents. The information potentially impacted included first and last name in combination with the individuals' Social Security number, education related information, and health information.

In response to this incident, District 47 took steps to secure their environment, conducted an investigation, and notified law enforcement. Additionally, District 47 began providing notice to the potentially impacted individuals on February 6, 2025, via U.S. mail. A copy of the notice is attached as **Exhibit A**. In an abundance of caution, District 47 is offering the potentially impacted individuals complimentary credit monitoring and identity protection services.

If you have any questions, please contact me.

Very truly yours,



Jason Goodwin, Esquire
CIPRIANI & WERNER, P.C.

Exhibit A



Return Mail Processing Center
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>

February 6, 2025

Dear <<First Name>> <<Last Name>>:

This letter to notify you of an incident that may have impacted some of your information as described below. At Crystal Lake Elementary District 47, we take privacy and security very seriously. At this time, there is no evidence to suggest that any information was subject to actual or attempted misuse as a result of this incident. However, out of an abundance of caution, we are providing you information about this incident, our response, and steps you can take to help protect your information, should you feel it is appropriate to do so.

What Happened:

On October 17, 2024, District 47 experienced a network disruption that affected certain district systems. Upon discovery, District 47 immediately took steps to secure the network and engaged a third-party firm to investigate the incident. Following a full and thorough investigation, we learned that certain information may have been accessed by an unauthorized third party in connection with this incident. On January 2, 2025, a review of the potentially affected data was completed identifying the information at risk and to whom it relates. We then worked to confirm appropriate contact information to provide you with this notice.

At this time, there is no indication that your information has been misused. However, we are providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel it is necessary to do so.

What Information Was Involved:

The information that could have been impacted may have included your first name or initial and last name, in combination with your <<Consolidated PII & PHI>>.

What We Are Doing:

We are committed to protecting the information in our care. Upon learning of this incident, we immediately took steps to secure our network and undertook a thorough investigation. Additionally, we are providing you access to <<12/24>> months of credit monitoring and identity protection services.

What You Can Do:

We recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change their passwords, take additional steps to protect your account, and notify

your financial institution or company if applicable. Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General. We have provided additional information below, which contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information:

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at our dedicated call center at 1-877-209-3329 Monday – Friday from 8 am – 8 pm Central Time. You can also write us at 300 Commerce Drive, Crystal Lake, Illinois 60014.

District 47 takes the security of information entrusted to our care very seriously. While it is regrettable this potential exposure occurred, please be assured that we are taking appropriate actions to rectify the situation and prevent such incidents in the future.

Sincerely,

Crystal Lake Elementary District 47

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

1. Website and Enrollment. Scan the QR image, go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. IDX representatives are available Monday through Friday from 8 am – 8 pm Central Time. Please note the deadline to enroll is May 6, 2025.

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 1-877-209-3329 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your 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 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.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. A police report is often required to dispute fraudulent items. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.