Return to IDX
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 1, 2021

RE: Notice of Data Breach

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

We are writing to inform you that the Stonington Public School District ("the District") was recently the victim of a cyber attack, which may have affected some personal information about you that the District maintains as a result of your current or former employment with the District, or status as a named dependent of a current or former employee of the District.

Here is what happened:

Early on the morning of September 27, 2021, we discovered unusual activity on certain computers at our organization and immediately began to take steps to protect our network and the information contained on it. Despite these steps, and based upon our subsequent investigation, we have reason to believe that the cyber attackers were able to evade our firewall, anti-virus program, and other network protections and potentially gain access to information maintained on two (2) file servers on our network. Our investigation determined that these two file servers were infected with a variant of ransomware virus, which encrypted the files on the two servers.

Based upon our investigation, the cyber attack occurred on September 25, 2021 and was contained within two (2) hours of our discovery of the incident early on the morning of September 27, 2021.

How the District responded:

Upon discovery of the cyber attack, the District's IT Director immediately took steps to protect the District's network and the information contained on it. We also engaged a third-party IT security firm to further investigate the incident and implement additional security protections to help prevent future incidents. In addition, we notified law enforcement officials of the incident.

We were able to recover complete and accurate copies of all affected files through our data back-up systems. Since that time, we have been working diligently to identify and contact those individuals with information affected by the incident.

Types of information involved:

Based upon our investigation, we have determined that the cyber attackers may have gained access to information stored on the two affected file servers. The affected files included certain historical employee data (including information regarding named dependents), which may have included the following information about you: name, date of birth, mailing address, telephone number, Social Security number, health insurance identification number, and wage and income tax information. Our investigation determined that our payroll system was not affected by the incident.

Protecting your information:

The District is taking this matter very seriously and is committed to ensuring your peace of mind.

To that end, we are offering identity theft protection services through IDX, the data breach and recovery services expert, **at no cost to you**, which includes credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. We are offering to provide this protection to you for a period of 24 months. To take advantage of this protection, please contact IDX to enroll in free identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6 am - 6 pm Pacific Time. Activate your coverage no later than February 1, 2022. We have also included some general educational information regarding protecting your identity in the enclosed "Reference Guide."

We sincerely regret that this incident occurred. If you have any questions, please call 860-572-0506 ext. 2152 during the hours of 10:00 a.m. to 2:00 p.m. or email us at gary.shettle@stoningtonschools.org.

Sincerely,

Gary J. Shettle
Director of Finance
Stonington Public Schools
40 Field Street
Pawcatuck, CT 06379

Reference Guide

We encourage individuals receiving the Stonington Public School District's letter dated November 1, 2021, to take the following steps:

Monitor Account Statements. Remember to look at your account statements regularly to be sure they are correct.

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC") website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open and bills you do not recognize. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The credit bureau will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing.

If you find items you don't understand on your report, call the relevant credit bureau at the number given on the report. Credit bureau staff will review your report with you. If the information can't be explained, then you will need to call the creditors involved. Information that can't be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Contact the U.S. Federal Trade Commission. If you detect any unauthorized transactions in your financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the FTC. If you believe your identity has been stolen, the FTC recommends that you take these additional steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft (including information about fraud alerts and security freezes):

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For a summary of your rights under the federal Fair Credit Reporting Act, please visit:
https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free fraud numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three credit bureaus. [*The table below contains the contact information relevant to fraud alerts*.]

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	877-478-7625	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, PA 19016	800-680-7289	www.transunion.com

Place a "Security Freeze" on Your Credit File. You also may wish to place a "security freeze" (also known as a "credit freeze") on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. There is no longer a fee for placing, lifting, and/or removing a security freeze. Unlike a fraud alert, you must place a security freeze on your credit file at each credit bureau individually. Since the instructions for establishing a security freeze differ from state to state, please contact the three national credit bureaus to find out more information. [*The table below contains the contact information relevant to security freezes*.]

Equifax	P.O. Box 105788 Atlanta, Georgia 30348	877-478-7625	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	888-397-3742	www.experian.com
TransUnion	Attn: Security Freeze P.O. Box 160 Woodlyn, PA 19094	888-909-8872	www.transunion.com

The credit bureaus may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Your complete address including proof of current address, such as current utility bill or telephone bill
- If you have moved in the past five (5) years, give your previous addresses where you have lived for the past five years
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Additional Information for New York Residents.
You can also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office:

New York State Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755
https://ag.ny.gov/internet/privacy-and-identity-theft

Additional Information for Rhode Island Residents.
Under Rhode Island law, you have the right to file a police report regarding this incident and obtain a copy of it.

You can contact the Rhode Island Attorney General to learn more about how to protect yourself from becoming a victim of identity theft:

Office of the Rhode Island Attorney General
Consumer Protection Unit
150 South Main Street
Providence, RI 02903
(401) 274-4400
consumers@riag.ri.gov
http://www.riag.ri.gov