



MULLEN
COUGHLIN

STATE OF NH
DEPT OF JUSTICE
MARCH 10 2017 10:32

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 10, 2017

VIA U.S. MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Foster:

We represent Glastonbury Public Schools (“Glastonbury”), 628 Hebron Avenue, Building 2, Glastonbury, Connecticut 06033, and are writing to notify your office of an incident that may affect the security of personal information relating to one (1) New Hampshire resident. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Glastonbury does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

Glastonbury was the victim of an email spoofing attack on February 17, 2017, by an individual pretending to be a Glastonbury payroll employee. A request was made from what appeared to be a legitimate Glastonbury email address for all 2016 Glastonbury employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before the company discovered that the request was made from a fraudulent account. Glastonbury discovered the fraudulent nature of the request on March 3, 2017 and has been working tirelessly to investigate and to mitigate the impact of the attack.

Notice to New Hampshire Residents

On March 3, 2017, Glastonbury provided preliminary notice to current employees via email. A copy of this notice is attached here as *Exhibit A*. On March 3, 2017, Glastonbury providing preliminary notice to former employees via a written letter. A copy of the written letter is attached hereto as *Exhibit B*. On March 9, 2017, Glastonbury began providing written notice of this incident to all affected current and former employees, which includes one (1) New Hampshire resident. Written notice will be provided in substantially the same form as the letter attached here as *Exhibit C*.

Other Steps Taken and To Be Taken

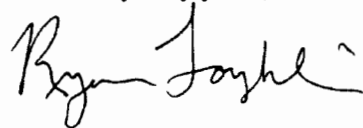
Upon discovering the fraudulent nature of the email, Glastonbury moved quickly to identify those that may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

Glastonbury is providing all potentially affected individuals access to 2 free years of credit and identity monitoring services, including identity restoration services, through AllClear ID, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Glastonbury is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Glastonbury is also providing written notice of this incident to other state regulators as necessary. Glastonbury has provided notice of this incident to the IRS and the FBI.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4786.

Very truly yours,

A handwritten signature in black ink, appearing to read "Ryan Loughlin", with a stylized flourish at the end.

Ryan C. Loughlin of
MULLEN COUGHLIN LLC

Exhibit A

----- Forwarded message -----

From: **Bookman, Alan** <bookmana@glastonburyus.org>

Date: Fri, Mar 3, 2017 at 3:28 PM

Subject: Important Information

To: All GPS <allgps@glastonburyus.org>

To All GPS Employees,

We have reason to believe that our district is the victim of the W-2 phishing scam that has impacted a number of school districts across the country. As a result, 2016 employee W-2 tax form information was compromised. W-2 forms contain an employee's name, address, social security number, and salary information. With the exception of Food Service personnel, any Glastonbury Public Schools employee who was issued a W-2 for the 2016 tax year could be affected.

Upon learning of the issue today, we immediately notified the FBI and the IRS. We also notified the Office of the Connecticut Attorney General and the Glastonbury Police Department. We are working with these agencies and our insurance company to provide safeguards to protect all GPS employees. More information on these services will be shared as soon as possible.

Please know that we are urgently taking all available measures to minimize the impact to our employees. It is concerning and frustrating and I apologize for the inconvenience and stress this causes. Unfortunately, cyber crime has become a common occurrence and many organizations, companies, and employees are dealing with the impact of these criminal acts.

I will share further updates as soon as possible.

Alan

--

Brian P. Czapla

Director of Educational Technology

Glastonbury Public Schools

Glastonbury, CT USA

Exhibit B



Office of the Superintendent

628 Hebron Ave., Bldg. #2, Glastonbury, CT 06033

Tel: (860) 652-7951 Fax: (860) 652-7952

www.glastonburyus.org

March 3, 2017

To Former GPS Employees,

We have reason to believe that our district is the victim of the W-2 phishing scam that has impacted a number of school districts across the country. As a result, 2016 employee W-2 tax form information was compromised. W-2 forms contain an employee's name, address, social security number, and salary information. With the exception of Food Service personnel, any former Glastonbury Public Schools employee who was issued a W-2 for the 2016 tax year could be affected.

Upon learning of the issue today, we immediately notified the FBI and the IRS. We also notified the Office of the Connecticut Attorney General and the Glastonbury Police Department. We are working with these agencies and our insurance company to provide safeguards to protect all current and former GPS employees. More information on these services will be shared as soon as possible.

Please know that we are urgently taking all available measures to minimize the impact to our employees. It is concerning and frustrating and I apologize for the inconvenience and stress this causes. Unfortunately, cyber crime has become a common occurrence and many organizations, companies, and employees are dealing with the impact of these criminal acts.

I will share further updates as soon as possible.

Sincerely,

A handwritten signature in cursive script that reads "Alan B. Bookman".

Dr. Alan B. Bookman, Ph.D.
Superintendent of Schools

Exhibit C



Processing Center • P.O. BOX 141578 • Austin, TX 78714



00033
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 9, 2017

Dear John Sample:

I am writing to make you aware of a recent email spoofing attack that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? We recently discovered that our school district was the victim of an email spoofing attack on February 17, 2017, by an individual pretending to be a payroll employee. A request was made from what appeared to be a legitimate Glastonbury Public School email address for all 2016 Glastonbury Public Schools employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before we discovered that the request was made from a fraudulent account. We discovered the fraudulent nature of the request on March 3, 2017 and have been working tirelessly to investigate and to mitigate the impact of the attack.

What Information Was Involved? A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Glastonbury Public Schools has stringent security measures in place to protect the security of information in our possession. At this time, we do not believe that the individual who sent the fraudulent email accessed our computer network or that our IT systems were otherwise compromised by this attack. However, our IT team is assessing the security and soundness of our systems. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We have contacted the IRS and FBI and the relevant state Attorneys General.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.



01-02-3-00

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-836-9826 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-9826 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

The cost of this service will be paid for by Glastonbury Public Schools. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. You can review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 tax return as soon as possible.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-836-9826 (toll free), Monday through Saturday, 9:00 a.m. to 9:00 p.m. EDT.

Glastonbury Public Schools takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in black ink that reads "Alan B. Bookman" with a stylized flourish at the end.

Dr. Alan Bookman
Superintendent
Glastonbury Public Schools

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. 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
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington,



DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.



Processing Center • P.O. BOX 141578 • Austin, TX 78714



01641
TO THE ESTATE OF JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

March 9, 2017

To the Estate of John Sample:

I am writing to make you aware of a recent email spoofing attack that may affect the security of your personal information. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? We recently discovered that our school district was the victim of an email spoofing attack on February 17, 2017, by an individual pretending to be a payroll employee. A request was made from what appeared to be a legitimate Glastonbury Public School email address for all 2016 Glastonbury Public Schools employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before we discovered that the request was made from a fraudulent account. We discovered the fraudulent nature of the request on March 3, 2017 and have been working tirelessly to investigate and to mitigate the impact of the attack.

What Information Was Involved? A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. Glastonbury Public Schools has stringent security measures in place to protect the security of information in our possession. At this time, we do not believe that the individual who sent the fraudulent email accessed our computer network or that our IT systems were otherwise compromised by this attack. However, our IT team is assessing the security and soundness of our systems. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We have contacted the IRS and FBI and the relevant state Attorneys General.

As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.



01-02-4-00

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-836-9826 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Credit Monitoring: This service offers additional layers of protection including credit monitoring and a \$1 million identity theft insurance policy. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-836-9826 using the following redemption code: Redemption Code.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

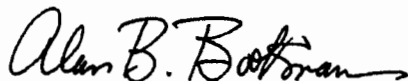
The cost of this service will be paid for by Glastonbury Public Schools. It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. You can review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 tax return as soon as possible.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-836-9826 (toll free), Monday through Saturday, 9:00 a.m. to 9:00 p.m. EDT.

Glastonbury Public Schools takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

A handwritten signature in cursive script that reads "Alan B. Bookman". The signature is written in black ink and includes a long, sweeping horizontal stroke at the end.

Dr. Alan Bookman
Superintendent
Glastonbury Public Schools

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. 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
1-800-685-1111
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington,



DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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 crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.