



40 North Main Street, Suite 1700
Dayton, OH 45423-1029
Tel: 937.228.2838 | Fax: 937.228.2816
taftlaw.com

SCOT GANOW
937.641.2041
sganow@taftlaw.com

RECEIVED

DEC 18 2020

December 16, 2020

CONSUMER PROTECTION

VIA FEDERAL EXPRESS

Attorney General Gordon MacDonald
New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident -Toledo Public Schools

Dear Mr. MacDonald:

Our client, Toledo Public Schools ("TPS") is providing this notice of a security incident as required under New Hampshire Revised Stat. Ann. §359-C:20, et. seq.

On September 8, 2020, TPS learned of a cyberattack that disrupted access to TPS learning systems and other TPS systems (the "Incident"). In response to the Incident, TPS immediately contacted the Federal Bureau of Investigation and engaged a forensic investigation firm. TPS took systems offline and worked with its forensic firm to secure its system, including implementing end point monitoring systems and conducting other analysis to ensure systems were secure before bringing data and limited systems back on line. Based on its investigation, TPS learned the attack was made possible through malicious software that appears to have been initiated by an email phishing scam. TPS has taken steps to secure the information in its systems, address the root cause of the incident, and improve its information security practices to better protect against a recurrence of this type of incident in the future.

On October 16, 2020, additional information came to the administration's attention that indicated the Incident may have also contributed to the unauthorized access and disclosure of student and employee personal information ("Unauthorized Disclosure") online. In response to this information, TPS immediately provided a preliminary update to students and employees of these developments via email and on the TPS website. Since the Unauthorized Disclosure, TPS has been analyzing the impacted files to better understand what personal information was potentially at risk, and providing notice to individuals and authorities, as applicable.

Attorney General Gordon MacDonald

December 16, 2020

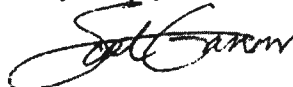
Page 2

Upon learning of the Unauthorized Disclosure, TPS immediately began reviewing the files that were alleged to have been taken from TPS systems. On December 4, 2020, TPS confirmed that the personal information of three (3) New Hampshire residents may have been impacted. TPS has been working since then to confirm the individuals, states of residence, and data at risk.

TPS will be providing written notification to 3 New Hampshire residents in substantially the same form as the document enclosed with this letter. The enclosed letter provides a brief description of the Incident, the information compromised, information about TPS's response to the Incident, and steps consumers can take to protect themselves. These written notices will be mailed to affected individuals during the week of December 14, 2020, and we anticipate New Hampshire residents will receive the notice by approximately December 19, 2020.

Should you have any questions about this matter, please do not hesitate to contact me.

Very truly yours,



Scot Ganow

Enclosure

28446677v1

[Date]

[First Name Last Name]

[Address]

[City, State Zip]

RE: Notification of Security Incident and Potential Disclosure of Personal Information

Dear [First Name],

Toledo Public Schools (“TPS”) takes the security and protection of your personal information seriously. You are receiving this letter as a current or former employee of TPS. We are providing you this letter to make you aware of a security incident that may have resulted in the unauthorized disclosure or access to your personal information. We are providing this letter and update out of an abundance of caution and in accordance with applicable laws to further share information with you so that you can better protect yourself.

What Happened

On September 8, 2020, TPS learned of a cyberattack that disrupted access to TPS learning systems and other TPS systems (the “Incident”). In response to the Incident, TPS immediately contacted the Federal Bureau of Investigation and engaged a forensic investigation firm. Based on its investigation, TPS learned the attack was made possible through malicious software that appears to have been initiated by an email phishing scam. In the weeks following the Incident, TPS and its forensics firm worked to secure all systems, remediate any risks, and successfully and securely bring its systems back online.

On October 16, 2020, additional information came to the administration’s attention that indicated the Incident may have also contributed to the unauthorized access and disclosure of your personal information (“Unauthorized Disclosure”) online. In response to this information, we immediately updated students, parents, and employees of these developments via email and on the TPS website. Since the Unauthorized Disclosure, TPS has been analyzing the impacted files to better understand what personal information was potentially at risk and providing notice to individuals and authorities, as applicable. Depending on your affiliation with TPS, you may have already received a notice similar to this one.

What Information Was Involved

At this time, we are unable to confirm how many individuals may have been affected by this Incident and Unauthorized Disclosure, and we cannot confirm or deny whether your personal information was acquired as a result of the Incident and Unauthorized Disclosure. Based on our investigation to date, we can only report that the personal information that could have been potentially accessed or viewed as a result of the Unauthorized Disclosure may have included, but was not necessarily limited to, the following data:

- first, middle, and last names for students, employees or parents/legal guardians;
- postal address;
- Social Security number;
- Driver's License number;
- phone numbers (home, work, cell);
- student ID number;
- race;
- gender;
- date of birth;
- grade of student and school attended;
- Individualized Education Plan information;
- special education information; and
- bank account number and routing number (e.g., employee direct deposit).

What We Did and What We Are Doing

Upon learning of the Incident in September, TPS engaged a third-party forensic investigation firm to identify the scope of the Incident and to assist us with securing our systems and data. TPS communicated with law enforcement to both report the Incident and assist investigators in working to identify the perpetrator(s) and any existing threats. TPS has slowly and carefully brought its systems back online and TPS continues to closely monitor its network and information systems for unusual activity, and strategically reduce network operations to minimize risk exposure to future incidents.

Upon learning of the Unauthorized Disclosure, as stated above, TPS immediately provided updates to its students and parents, as well as its employees that might have been impacted. In addition to this notice, we are providing notice to the credit bureaus. We are actively reviewing the files alleged to have been taken from TPS to determine the scope of the Unauthorized Disclosure. To the best of our knowledge and efforts, TPS has not experienced any other incidents that we believe impact the security of our TPS information or systems since executing our remediation plan in September of this year. TPS is continuing its investigation and due diligence, including engaging additional resources and experts and evaluating the extent of risk to personal information, and is working to continue to improve its practices and systems to prevent another attack, disruption of services, or disclosure of information.

What You Can Do

At this time, there is nothing you have to do in response to this letter. In addition to the notices and suggestions we have previously provided, please be vigilant about monitoring your personally identifiable information, in particular your credit report information and financial accounts, to protect against fraudulent activity.

In the meantime, out of an overabundance of caution, we are providing this notice and complimentary identity theft and credit monitoring services to our past and present employees. To take advantage of these services, please follow these steps.

1. Call TPS at (419) 671-0242 to receive your Personal Verification Code; and
2. Go online and register at the following website: <https://secure.identityforce.com/benefit/tps> by [DATE].

Step 1: Enter your first and last name

Step 2: Enter your email address

Step 3: Enter your Personal Verification Code

Step 4: Click Continue button

Step 5: Enter the required information on the Personal Information Page

We sincerely regret this has transpired and any concerns it has caused. If you have concerns about identity theft, you can contact local law enforcement and file a police report. You can also contact your state's Attorney General, as well as the Federal Trade Commission or one of the credit bureaus for more information about how to protect your identity.

For More Information:

You can place a fraud alert, place a security freeze, or order a free credit report by contacting any of the following credit bureaus at one of the phone numbers listed below or visiting their respective websites. Please refer to each credit bureau's instructions when making any such requests.

Equifax
1-888-548-7878
P.O. Box 740256
Atlanta, GA 30348
www.equifax.com

Experian
1-888-397-3742
P.O. Box 4500
Allen, TX 75013
www.experian.com

Trans Union
1-888-909-8872
P.O. Box 2000
Chester, PA 19022
www.transunion.com

Security Freezes. You can place a security freeze with the credit bureaus free of charge. Under state law, a security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without written authorization. However, please be aware 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.

Fraud Alerts. You can place a fraud alert with the credit bureaus free of charge. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Credit Reports. You can request that all three credit reports be sent to you, free of charge, for your review. 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. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

The FTC provides more information about how to protect your identity at either <https://www.ftc.gov/> or <https://www.identitytheft.gov/>. You may also find additional information on any applicable rights under the Fair Credit Reporting Act. You can also contact the FTC by using the information below.

Federal Trade Commission
1-202-326-2222
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580

For District of Columbia Residents: You may also contact the Attorney General for the District of Columbia for more information about how to protect your identity by using the information below:

Attorney General Karl A. Racine
400 6th Street, NW
Washington, DC 20001
Phone: (202) 727-3400
Website: <https://oag.dc.gov/>

For Maryland Residents: You may also contact the Maryland Attorney General's Office for more information about how to protect your identity by using the information below:

Attorney General Brian E. Frosh
200 St. Paul Place
Baltimore, MD 21202
Phone: 410-528-8662
Website: <https://www.marylandattorneygeneral.gov/>

For New York Residents: You may also contact the New York Attorney General's Office for more information about how to protect your identity by using the information below:

Attorney General Letitia James
Toll Free Phone Number: (800) 771-7755
Website: <https://ag.ny.gov/>

For North Carolina Residents: You may also contact the North Carolina Attorney General's Office for more information about how to protect your identity by using the information below:

Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
Toll Free in NC: 1-877-566-7226
Outside NC: 919-716-6000
Website: <https://ncdoj.gov>

For Rhode Island Residents: You may also contact the Rhode Island Attorney General's Office for more information about how to protect your identity by using the information below:

Attorney General Peter F. Neronha
Toll Free Phone Number: (401) 274-4400
Website: <http://www.riag.ri.gov/>

Again, we sincerely regret that this has occurred. If you have any additional questions, please call 1-877-694-3367.

Sincerely,

[TPS Official Name, Title]