

RECEIVED

DEC 10 2020

Lauren C. Ostberg, Attorney  
direct: 413-272-6282  
fax: 857-800-8249  
lostberg@bulkley.com

CONSUMER PROTECTION

December 7, 2020

**VIA CERTIFIED MAIL, RETURN RECEIPT REQUESTED**

Consumer Protection Bureau  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

**RE: Unauthorized access of personal information at Springfield Public Schools**

Dear Attorney General MacDonald:

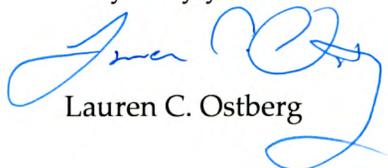
Pursuant to N.H. Rev. Stat. § 359-C:20, and on behalf of our client Springfield Public Schools ("SPS"), of 1550 Main Street in Springfield, Massachusetts, we are writing to notify you of a possible unauthorized access of personal information involving approximately 9 New Hampshire residents.

The incident apparently began on October 1, 2020, when attackers likely first accessed SPS's servers by compromising an endpoint. They then brute force attacked the server and installed a brand-new iteration of malware, and triggered the payload at 3:21 a.m. on October 8, 2020. SPS was able to interrupt the incident approximately five hours later.

Since the incident, SPS has incrementally rebuilt servers from backup on more secure settings, while consistently scanning for "fingerprints" of the attackers. SPS has also rebuilt its student and staff VPN—critical in a period of remote education—with significantly limited access. SPS continues to rely on the advice of specialists, particularly the Multi-State Information Sharing and Analysis Center, in securing its system against future, novel attacks.

On November 13, 2020, SPS first identified residents of New Hampshire whose information, including their social security numbers, may have been indexed or accessed. Those residents were informed by letter, an example of which is attached, mailed on December 3, 2020. The attached press release was submitted to the *New Hampshire Union Leader* on December 3, 2020 as well. Should you need additional information, please contact me.

Very truly yours,



Lauren C. Ostberg

Enclosures  
3390769v1



To Enroll, Please Call:  
833-905-3224

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

Enrollment Code: [XXXXXXXXXX]

[Date]

## NOTICE OF DATA BREACH

Dear [Resident]:

**What happened:** We are writing to inform you that your personal information stored on the Springfield Public Schools' servers may have been accessed by an unauthorized individual in October 2020. An attacker gained access to Springfield Public Schools' network on or around October 1, 2020; on October 8, 2020, the attacker attempted to download information from our servers. We were able to interrupt the incident that day.

**What information was involved:** On or after Friday, November 13, 2020, we determined that your social security number, your driver's license number, and/or, in rare cases, your credit card information, may have been accessed in that attack.

**What we are doing:** We understand that your information is important, and we regret that this has occurred. Since the incident, we have been working cooperatively with law enforcement and an organization endorsed by the Department of Homeland Security to investigate the incident, restore systems that were taken offline as a result of this attack, and recalibrate our scanning tools to detect previously undetectable intrusions into our network, among other enhanced security measures.

**What you can do:** Because your social security number may have been exposed in this incident, we would like to offer you twenty-four months of complimentary credit monitoring. We are also offering CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services through IDX. We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 833-905-3224 and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. As of today's date, we are aware of no evidence indicating that your personal information has been misused. Still, we encourage you to remain vigilant and monitor your account statements and free credit reports. Federal law currently allows consumers to place a security freeze on their credit reports, free of charge. More detailed information on that process, and other resources to protect your identity, are appended to this letter.

**For more information:** If you should have any further questions, please contact 833-905-3224 or go to <https://app.idx.us/account-creation/protect>. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

Sincerely,

**SPRINGFIELD PUBLIC SCHOOLS**

## Other important information

Federal law currently allows consumers to place a security freeze on their credit reports free of charge. A security freeze prohibits a credit reporting agency 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. Credit reporting agencies are not permitted to charge you to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax ([www.equifax.com](http://www.equifax.com)); Experian ([www.experian.com](http://www.experian.com)); and TransUnion ([www.transunion.com](http://www.transunion.com)) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Trans Union Security Freeze Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19022-2000
---	--	--

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
1. Social Security Number;
2. Date of birth;
3. The address[es] where you have lived over the prior five years;
4. Proof of current address such as a current utility bill or telephone bill;
5. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
6. Social Security card, pay stub, or W2
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

You can obtain additional information about the steps you can take to avoid identity theft from the following agencies, or your state attorney general. Some of their contact information is below. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. If you believe you are the victim of identity theft, you should report it to local law enforcement or your attorney general.

**California Residents:** Visit the California Office of Privacy Protection ([www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)) for additional information on protection against identity theft.

**DC Residents:** Office of the Attorney General of the District of Columbia, 400 6<sup>th</sup> Street, NW, Washington, DC 20001, 202-727-3200 [oag.dc.gov/consumer-protection](http://oag.dc.gov/consumer-protection)

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**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. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201904\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201904_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.

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

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400. You should know that 9 Rhode Island residents were potentially impacted by this breach of data security.

**All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft), 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.



News Release  
For Immediate Release

## **SPS Offers Free Credit Monitoring Following Cyber Attack on IT Network**

December 3, 2020 - Springfield Public Schools (SPS) is offering two years of free credit monitoring to some current and former employees and a small number of job applicants following a cyberattack that occurred on its computer network this fall.

Superintendent of Schools Daniel Warwick said the move is taken as a cautionary measure to help protect against any breach to the security of personal information that may have occurred because of the cyberattack.

"We sincerely regret that this event would cause concern and we are doing all we can, going above and beyond, to offer services free of charge to help them enhance the protection of their private information and hopefully provide some peace of mind," Warwick said, adding that the district is providing two years of free credit monitoring; two years of monitoring for data appearing on the dark web; assistance with identity recovery if needed; and identity theft insurance for individuals whose personal information may have been compromised.

Today, the district mailed letters to those individuals whose personal information may have been compromised. Those who do not receive a letter are not believed to have had their personal information possibly compromised.

The security incident occurred after hackers attacked the district's network on the morning of October 8<sup>th</sup>. The attack, which caused a cancellation of remote learning for the day, was an attempt to encrypt all SPS network data and extract data with sensitive information. The network was protected to industry-standard; had a fully updated firewall; and was covered with intrusion detection and malware tools. However, the attack relied on a new version of malware that was not detectable by current tools, and which was only identified after assistance from the Federal Bureau of Investigation and a cybersecurity resource endorsed by the Department of Homeland Security.

The SPS Information Technology (IT) department interrupted the attack by shutting down the network, which is what prompted the cancellation of remote education for the day. The IT team then prioritized restoring data and remote learning services. Today, the IT department remains focused on ensuring the security of the network and the continual restoration of data and services from the backup system. Additionally, the team, in partnership with law enforcement, is investigating the source of the attack. That investigation recently determined that the data of some current and former employees may have been compromised, causing the district to notify those whose information the attackers may have accessed via mail this week.

"We'd seen districts throughout the country grapple with cyberattacks, so we were extremely diligent and proactive in implementing layers of defense, but unfortunately, we live in a world where no protective measure is 100 percent effective against cyber threats," said Chief of information Technology Paul Foster.

Since the attack, the district's network security has been further enhanced, additional security practices and protocols have been put in place, and the district's cybersecurity partners will continue to provide further recommendations to the district. Warwick said the district is poised to devote the necessary resources to help protect its IT system from further attack and to providing as many protective resources as possible in response to the October 8<sup>th</sup> attack.

If you believe your information may have been compromised in this cyberattack, please call 833-905-3224 to enroll in credit monitoring services. To learn more about your rights under Massachusetts and federal law, please visit the district's website at:

[https://www.springfieldpublicschools.com/news/news/free\\_credit\\_monitoring\\_following\\_cyber-attack](https://www.springfieldpublicschools.com/news/news/free_credit_monitoring_following_cyber-attack)

(END)