GOODWIN

David S. Kantrowitz
+1 617 570 1254
DKantrowitz@goodwinlaw.com

Goodwin Procter LLP
100 Northern Avenue
Boston, MA 02210
goodwinlaw.com
+1 617 570 1000

November 16, 2020

BY FEDEX

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

RE: NOTICE OF DATA SECURITY INCIDENT

Dear Sir/Madam:

We write on behalf of UniFirst Corporation ("UniFirst") to notify you of a data security incident that UniFirst recently experienced. Specifically, on or around September 28, 2020, an unauthorized person gained access to email inboxes belonging to a small number of UniFirst employees. As a result, the intruder may have viewed certain personal information in UniFirst's possession. UniFirst discovered the incident and shut down the access on September 29, 2020, and recently completed its review to determine those who are potentially affected.

After discovering the incident, UniFirst worked to determine the nature and scope of the access and ensure it was contained. The information potentially accessed includes name, Social Security number, and date of birth. While the file was encrypted and UniFirst does not have conclusive evidence it was accessed, UniFirst notified 10 New Hampshire individuals of the incident on October 13, 2020 as a precaution. At this time UniFirst does not have any evidence that any individual has suffered from identity theft as a result of the incident.

UniFirst took prompt action to assist the New Hampshire residents who may be impacted by this event. UniFirst notified the residents, and recommended actions they can take to protect themselves, such as monitoring account statements, obtaining credit reports, and instituting a security freeze on their credit files. UniFirst also made available 24 months of identity protection services from PrivacyArmor by InfoArmor, at no cost to the individual. A copy of the notice sent to the individuals is attached to this letter. UniFirst is undertaking a review of its systems to help guard against a similar incident occurring in the future.

Thank you for your attention to this matter.

Sincerely,

David S. Kantrowitz

David S. Kantrowitz

UniFirst

Memo

October 13, 2020

Re: Privacy Breach Communication

We are providing this communication to let you know that UniFirst became aware of a privacy breach that occurred within our organization that could potentially involve your personal information.

We learned that through a phishing email attack, credentials to a specific mailbox were given, providing complete access to the email account. As soon as we were made aware, IT went through the appropriate protocol of conducting a deep scan and was able to clean the breach. In addition, we immediately engaged with a forensic company to conduct a detailed analysis on the compromised mailbox. At this time, we are unclear as to what emails were accessed. However, we know there was an encrypted file in the inbox that included your full name, social security number, and date of birth. Although the file was encrypted, the password to access the file was included in a separate email also in the inbox.

To help ensure that this information is not used inappropriately, if it were to be the case that the file in question was accessed, UniFirst will cover the cost for you to receive credit monitoring for one year. We have partnered with Allstate Identity Protection through our voluntary benefit offering to provide you this solution. We will provide the appropriate information to Willis Towers Watson, our benefits administrator platform to auto enroll you. If we identify that you currently have coverage on an employee paid basis, we will work to have those payroll deductions turned off. You should receive communication on this enrollment within the next couple of weeks.

In addition, we highly advise you review and take some or all of the steps below to protect yourself from potential harm from the breach.

- **Place a fraud alert on your credit report.** A fraud alert tells creditors to contact you before they open any new credit accounts or change your existing accounts. This can help prevent an identity thief from opening additional accounts in your name. As soon as one of the credit bureaus confirms your fraud alert, the other two credit bureaus will be automatically notified in order to place alerts on your credit report, and all three reports will be sent to you free of charge. To place a fraud alert on your credit file,

contact one of the three national credit bureaus at the following numbers, or you can visit their websites for further information.

- Equifax: 1- 866-349-5191; www.equifax.com
- Experian: 1-888-397-3742; www.experian.com
- TransUnion: 1-800-680-7289; www.transunion.com

- **Monitor your credit reports.** By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report(s). You should review your credit reports and other account statements over the next 12 to 36 months. Immediately report any suspicious activity to the credit bureaus.

  Legally the three credit reporting companies must provide you a free copy of your credit report, at your request, once every 12 months. Even if your data has not been involved in a breach, periodic monitoring of your credit reports is a recommended best practice.

- **Place a "credit freeze" on your credit file** so that no credit reports can be released without your approval. Please contact the three national credit bureaus for more information. All bureaus charge a fee for this service.

We take our role in protecting your personal information and using it in an appropriate manner very seriously. Please rest assured that we are doing everything we can to rectify the situation.

Should you have any questions regarding this communication, please do not hesitate to contact me.

Sincerely,

Denise Valentin-Diaz

978-658-8888 ext.4364

Denise_Valentin@UniFirst.com