April 29, 2021

VIA FIRST CLASS MAIL and E-MAIL

New Hampshire Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: attorneygeneral@doj.nh.gov

To Whom It May Concern:

Festo Corporation ("Festo") is notifying the New Hampshire Office of the Attorney General with respect to an incident involving the potential exposure of personally identifiable information ("PII") for nine (9) New Hampshire individuals, as described below.

1. Nature of the event

Festo has had two-factor authentication in place for the Microsoft 365 environment for many years. On March 4th, 2021, Festo determined that an employee had fallen victim to a phishing attack at some time in January 2021 (estimated). Through the phishing attack, the employee inadvertently disclosed credentials to access her Festo email account. During the period starting from February 17 and ending on February 24, 2021 (the "Period"), Festo had to turn off its two-factor authentication software in connection with the migration of its phone authentication system. Accordingly, at some point during the Period, a malicious actor gained access to the employee's Microsoft 365 online account, including her email account.

Pamela Weinsaft
General Counsel
Festo Corporation
1377 Motor Parkway
Suite 310
Islandia, NY 11749
Phone: (631)404-3346
Pamela.Weinsaft@festo.com

***2.* Number of New Hampshire consumers affected**

Based on the investigation, nine (9) New Hampshire individuals were affected. A formal notification letter will be sent to the individuals on April 30th via regular mail. A copy of the notification letter is included with this letter.

3. Information potentially compromised

Based on the investigation, photographs of the New Hampshire individuals' driver's licenses, which were saved in an email folder, may have been compromised.

4. Steps taken and plans relating to the event

Upon learning that a Festo email account may have been compromised, Festo immediately began an investigation to determine whether the potential compromise occurred and whether the employee had access to any PII. On the basis of the investigation, Festo determined that the employee had in fact fallen victim to a phishing incident and that the

FESTO

New Hampshire individuals. However, Festo's investigation uncovered no evidence of unauthorized access to Festo's system (and thus, no unauthorized access of the PII).

Festo has taken steps to ensure that its employees comply with the company's policies and procedures to protect against phishing incidents. This includes maintaining its two-step authentication software, holding annual trainings on how to identify phishing emails, and providing technical notifications to flag potentially unreliable email communications. Moreover, Festo has technical processes and IT security staff in place to monitor for potentially dangerous email traffic. Festo has also ensured that the all United States employees change their credentials for email access.

Due to the abovementioned steps taken, Festo believes that there is no further risk of additional exposure. In addition, for the same reasons, Festo believes that the misuse of PII is not reasonably likely to have occurred.

5. Contact information

If you have any additional questions, please contact me at pamela.weinsaft@festo.com or at (631) 404-3346 during business hours.

Sincerely,

Pamela Weinsaft
General Counsel

FESTO

C/O 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>>

April 30, 2021

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

What Happened
In March, Festo determined that an employee had fallen victim to a phishing attack at some time in January 2021 (estimated). Through the phishing attack, the employee inadvertently disclosed credentials to access her Festo email account. During the period starting from February 17 to February 24, 2021 (the "Period"), a malicious actor gained access to the employee's Microsoft 365 online account, including her email account and all the folders to which she had access via the OneDrive.

What Information Was Involved
After a review of all the affected inboxes and folders, Festo has determined that the intruder had potential access to a photo copy of your driver's license, which includes name, date of birth, home address and license number. There is no evidence to suggest that there has been any attempt to misuse any of the information.

What We Are Doing
Festo has taken steps to ensure that its employees comply with the company's policies and procedures to protect against phishing incidents. This includes utilizing two-step authentication software, holding annual trainings on how to identify phishing emails, and providing technical notifications to flag potentially unreliable email communications. Moreover, Festo has technical processes and IT security staff in place to monitor for potentially dangerous email traffic. Festo has also ensured that the victim-employee change her credentials for email access. Due to the abovementioned steps taken, Festo believes that there is no further risk of additional exposure. In addition, for the same reasons, Festo believes that the misuse of PII is not reasonably likely to have occurred That said, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of 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.

What You Can Do
We encourage you to contact IDX with any questions and 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. Please note the deadline to enroll is July 30, 2021.

Again, at this time, there is no evidence that your information has been misused. However, if you do not already have identity protection as one of your Festo benefits, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information
You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call 1-800-939-4170 or go to https://app.idx.us/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Pamela Weinsaft
General Counsel

(Enclosure)

Recommended Steps to help Protect your Information

1. **Website and Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. **Telephone.** Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. **Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity 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 you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. **Place Fraud Alerts** with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

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

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, 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, 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. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_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, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, 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, Telephone: 401-274-4400

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