



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

JUN 01 2020

CONSUMER PROTECTION

Edward J. Finn
Office: 267-930-4776
Fax: 267-930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 27, 2020

VIA U.S. MAIL

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

Re: Notice of Data Event

Dear Sir or Madam:

We represent Symbotic LLC (“Symbotic”), located at 200 Research Drive, Wilmington, MA 01887, and are writing to notify your office of an incident that may affect the security of some personal information relating to three (3) New Hampshire residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Symbotic does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On April 26, 2020, Symbotic became aware of suspicious activity relating to our systems and immediately launched an investigation, with the assistance of outside computer forensics specialists, to determine the nature and scope of the activity. The investigation determined an unauthorized actor accessed Symbotic’s system and acquired certain data. This unauthorized access and acquisition of data occurred on or around April 26, 2020. On or around May 14, 2020, the threat actor posted personal data belonging to certain employees on the website Mega.nz. After take down requests, the site took the data down on May 15, 2020.

Symbotic notified the FBI and continues to support the FBI’s investigation.

The information that could have been subject to unauthorized access includes name, address, and Social Security number.

Notice to New Hampshire Residents

On or about May 26, 2020, Symbotic provided written notice of this incident to all affected individuals, which includes three (3) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

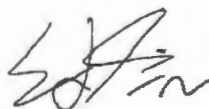
Upon discovering the event, Symbotic moved quickly to investigate and respond to the incident, assess the security of Symbotic systems, and notify potentially affected individuals. Symbotic worked quickly, with a number of third-party specialists, to secure its systems and implement additional network and endpoint monitoring. Symbotic is providing access to credit monitoring services for 18 months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Symbotic is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Symbotic is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, 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.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4776.

Very truly yours,



Edward J. Finn of
MULLEN COUGHLIN LLC

EJF:brb
Enclosure

EXHIBIT A



SYMBOTIC LLC
200 Research Drive
Wilmington, MA 01887

[Date]

[First Name] [Last Name]
[Address #1]
[Address #2]
[City, State Zip Code]

Dear [First Name] [Last Name]:

Symbotic LLC (“Symbotic”) is writing to notify you of a recent data security incident that has impacted the security of some of your personal information. Although at this time there is no indication that your information has been fraudulently misused in relation to this incident, we are providing you with information about the incident, our response to it, and information about how you can better protect your personal information from any threat, should you feel it appropriate to do so.

What Happened? On April 26, 2020, Symbotic became aware of suspicious activity relating to our systems and immediately launched an investigation, with the assistance of outside computer forensics specialists, to determine the nature and scope of the activity. The investigation determined an unauthorized actor accessed Symbotic’s system and acquired certain data. This unauthorized access and acquisition of data occurred on or around April 26, 2020.

Our investigation is ongoing; however, at this time, we believe that files containing your information were acquired by the unauthorized actor. The unauthorized actor threatened to release, and did release, files acquired from our network, which contain your data; however, we are unaware of any actual fraudulent misuse of your personal information. These files were posted on an upload site on May 14, 2020. We are working with law enforcement will be contacting the sire to demand the information be removed.

What Information Was Involved? Our investigation determined that your name and [Data Elements] were stored within a file that was acquired by the unauthorized actor.

What We Are Doing. The confidentiality, privacy, and security of your personal information are among our highest priorities, and we have strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems and investigate the incident. Symbotic worked quickly, with a number of third-party specialists, to secure its systems and implement additional network and endpoint monitoring. We also notified the FBI and are working closely with them.

As you know from our prior email, Symbotic has offered you access to twelve (12) months of complementary credit monitoring services through Kroll. We will be increasing that offering to eighteen (18) months through Kroll.

What Can You Do. Please review the enclosed “Steps You Can Take to Help Protect Your Information,” which contains information on what you can do to better safeguard against possible misuse of your information.

For More Information. We understand that you may have questions about this incident that are not addressed in this notice. If you have additional questions or concerns, please contact Kate Eastman at keastman@symbotic.com.

We sincerely regret the inconvenience this event may cause you. We remain committed to safeguarding the information in our care and will continue to take steps to ensure the security of our systems.

Sincerely,

A handwritten signature in black ink, appearing to read "Kate Eastman". The signature is fluid and cursive, with a prominent initial "K" and "E".

Kate Eastman
Director, Total Rewards
Symbotic LLC

Steps You Can Take to Protect Your Information

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports 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.

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

**P.O. Box 9554
Allen, TX 75013
1-888-397-3742**

www.experian.com/freeze/center.html

TransUnion

**P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872**

www.transunion.com/credit-freeze

Equifax

**P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111**

www.equifax.com/personal/credit-report-services

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.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
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.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, 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 report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.