FOLEY
FOLEY & LARDNER LLP

ATTORNEYS AT LAW
777 EAST WISCONSIN AVENUE
MILWAUKEE, WI 53202-5306
414.271.2400 TEL
414.297.4900 FAX
WWW.FOLEY.COM

WRITER'S DIRECT LINE
414.297.5864
jrathburn@foley.com EMAIL

CLIENT/MATTER NUMBER
016831-0810

September 29, 2017

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

Re: Notification Pursuant to N.H. Rev. Stat. § 359-C:20

Dear Office of the Attorney General:

We are writing on behalf of our client, Briggs & Stratton Corporation (Briggs), to notify you of a breach of security involving seven (7) New Hampshire residents.

NATURE OF THE UNAUTHORIZED DISCLOSURE

Briggs experienced a malware attack on Briggs' computer systems at its Milwaukee, Wisconsin and Munnsville, New York locations that potentially compromised information from approximately July 25, 2017 to July 28, 2017. Briggs became aware of this incident on July 25, 2017 and took immediate steps to both contain and thoroughly investigate the attack. Although Briggs has no evidence of actual misuse of any of information, it notified individuals out of an abundance of caution because the malware, by its nature, could have allowed a third party to access, use, and/or disclose individuals' account-related, human resources, and/or health plan information as listed on the sample copy of the notice enclosed.

After discovery of this incident, Briggs notified the Federal Bureau of Investigation, the Department of Homeland Security, and the Wisconsin Department of Justice. Due to the ongoing investigation, law enforcement requested that Briggs delay notifying individuals of the incident until September 30, 2017. Briggs complied with that request and mailed notifications to potentially affected individuals on September 29, 2017. Enclosed is a sample copy of the notice that is being provided to the individuals potentially affected.

STEPS WE ARE TAKING RELATED TO THE INCIDENT

In response to this incident, Briggs hired forensic consultants to eradicate the malware, determine if any information was compromised, and help Briggs prevent an incident like this from happening in the future. Briggs also provided potentially affected individuals with three (3) bureau credit monitoring and identity theft protection through Experian IdentityWorks at no cost to the individual for one (1) year.

If you have any further inquiries concerning this notification, please do not hesitate to contact me.

Sincerely,

Jennifer L. Rathburn

Encl: Sample Notification Letter

BRIGGS & STRATTON CORPORATION

September 29, 2017

NOTICE OF DATA BREACH

WHAT HAPPENED?

We value and respect the privacy of information which is why Briggs & Stratton Corporation (Briggs) is writing to follow up with you and your health plan dependents and insurance beneficiaries regarding a recent malware attack on Briggs' computer systems at its Milwaukee, Wisconsin and Munnsville, New York locations that potentially compromised information from approximately July 25, 2017 to July 28, 2017. We became aware of this incident on July 25, 2017 and took immediate steps to both contain and thoroughly investigate this attack. Although we have no evidence of actual misuse of any of your information, we are notifying you out of an abundance of caution because the malware, by its nature, could have allowed a third party to access, use, and/or disclose your information.

WHAT INFORMATION WAS INVOLVED?

Attached is a table identifying the type of information that could potentially have been involved in the malware attack based on your relationship with Briggs.

WHAT WE ARE DOING.

After discovery of this incident, we notified the Federal Bureau of Investigation, the Department of Homeland Security, and the Wisconsin Department of Justice. Due to the ongoing investigation, law enforcement requested that we delay notifying you of this incident until now.

In response to this incident, Briggs also hired forensic consultants to eradicate the malware, determine if any information was compromised, and help Briggs prevent an incident like this from happening in the future.

Because we are committed to protecting your information and the information of your health plan dependents and insurance beneficiaries, we have made arrangements to provide individuals with credit monitoring and identity theft services. You will automatically be provided with identity restoration services and may also opt to enroll in daily credit bureau monitoring. These services will be available to you for one year, at no cost to you. Attached to this notice for your convenience is more information and instructions on how to enroll.

WHAT YOU CAN DO.

We recommend that you consider taking advantage of the credit monitoring and identity theft services described above and that you also change your password(s) associated with any accounts you may have accessed using Briggs' computer systems at the Milwaukee, Wisconsin or Munnsville, New York locations during the timeframe of the potential compromise. Please also review the attachment to this letter (Steps You Can Take to Further Protect Your Information), which provides further information on ways you can protect your information.

FOR MORE INFORMATION.

Briggs sincerely regrets any inconvenience that this incident may have caused to you. If you have any questions, please call our dedicated Incident Response Line at 1-888-396-9514 or visit our webpage at https://www.basco.com.

Sincerely,

Briggs & Stratton Corporation

Steps You Can Take to Further Protect Your Information

Review Your Account Statements & Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant for incidents of fraud and identity theft by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission. To file a report with the FTC, go to www.ftc.gov/idtheft, call 1-877-ID-THEFT (877-438-4338), or write to the FTC Bureau of Consumer Protection, 600 Pennsylvania Ave., NW, Washington, DC 20580. Reports filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. A copy of Taking Charge: What to Do if Your Identity is Stolen, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at www.ftc.gov/bcp/edu/microsites/idtheft/.

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three (3) major credit reporting agencies once every twelve (12) months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three (3) national credit reporting agencies or enrolling in the Experian product as described on the page of this letter entitled "Information on Experian Services." Contact information for the three (3) national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alert

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least ninety (90) days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, please see the instructions from Experian on the page of this letter entitled "Information on Experian Services" or contact any of the three (3) credit reporting agencies identified above. Additional information is available at www.annualcreditreport.com.

Security Freeze

In some US states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each of credit reporting agencies listed above. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee to place, lift or remove the security freeze, which may vary by state. However, if you are a victim of identity theft and have filed a report with your local law enforcement agency or submitted an ID Complaint Form with the FTC, there may be no charge to place the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number,

date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Required Disclosures for Maryland and North Carolina Residents

For Maryland and North Carolina Residents
You can obtain information from these sources about preventing identify theft:

Federal Trade Commission:
Visit the Federal Trade Commission website at:
www.ftc.gov, or call 1-877-ID-THEFT
or write to this address:
Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, DC 20580

Maryland:
Visit the Maryland Office of the Attorney General, Identity Theft Unit at:
www.oag.state.md.us/idtheft/index.htm, or call 1-888-743-0023
or write to this address:
Maryland Office of the Attorney General
Identity Theft Unit
16th Floor
200 St. Paul Place
Baltimore, MD 21202

North Carolina:
Visit the North Carolina Office of the Attorney General at:
www.ncdoj.gov/Protect-Yourself/2-4-3-Protect-Your-Identity.aspx, or call 1-877-566-7226
or write to this address:
Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001

Required Disclosures for Massachusetts Residents

You have the right to obtain any police report filed in regard to this incident. Although we notified law enforcement of this malware attack, we did not file a police report at this time. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each 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 (3) credit reporting agencies listed on page 2 of this notice. 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 during the prior five (5) 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; and
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

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 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 (3) credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN 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.

Required Disclosures for New Mexico Residents

As a resident of New Mexico, you have certain rights under the New Mexico Fair Credit Reporting and Identity Security Act, New Mexico Code § 56-3A-1 *et seq*. You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity;
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report; and
4. Payment of a fee, if applicable.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen (15) minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three (3) business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen (15) minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three (3) major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

Information on Experian Services

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three (3) major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for one (1) year from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks [SM] as a complimentary one-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **12/31/2017** (Your code *will not work after this date.*)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcreditone
- Provide your **activation code**: **[insert]**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **12/31/2017**. Be prepared to provide engagement number **DB03555** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

---

[1]Offline members will be eligible to call for additional reports quarterly after enrolling.

[2]Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

POTENTIALLY AFFECTED INFORMATION TABLE

If you are . . .	**Then it's possible the following types of information may have been accessed, used and/or disclosed:**
A current Briggs employee located in Milwaukee, Wisconsin or Munnsville, New York	*If you participate in a health plan offered by Briggs:* (1) name; (2) Social Security number; (3) address; (4) dates related to you, such as date of birth; (5) telephone number; (6) driver's license number; (7) state identification number; (8) employee ID; (9) individual taxpayer identification number; (10) medical information and health insurance information, including health plan beneficiary number; (11) passport number; (12) work related evaluations; and (13) account log-in information, such as user names and email addresses with associated passwords, for Briggs' accounts and other accounts you may have accessed using Briggs' computer systems at the Milwaukee, Wisconsin or Munnsville, New York locations during the timeframe of the potential compromise.
	If you do not participate in a health plan offered by Briggs: (1) name; (2) Social Security number; (3) date of birth; (4) driver's license number; (5) state identification number; (6) employee ID; (7) individual taxpayer identification number; (8) passport number; (9) work related evaluations; and (10) account log-in information, such as user names and email addresses with associated passwords, for Briggs' accounts and other accounts you may have accessed using Briggs' computer systems at the Milwaukee, Wisconsin or Munnsville, New York locations during the timeframe of the potential compromise.
A current Briggs employee located somewhere other than Milwaukee, Wisconsin or Munnsville, New York Or A former employee, regardless of your location when you worked at Briggs	*If you participate in a health plan offered by Briggs:* (1) name; (2) Social Security number; (3) address; (4) dates related to you, such as date of birth; (5) telephone number; (6) driver's license number; (7) state identification number; (8) employee ID; (9) email address; (10) individual taxpayer identification number; (11) medical information and health insurance information, including health plan beneficiary number; (12) passport number; and (13) work related evaluations.
	If you do not participate in a health plan offered by Briggs: (1) name; (2) Social Security number; (3) date of birth; (4) driver's license number; (5) state identification number; (6) employee ID; (7) individual taxpayer identification number; (8) passport number; and (9) work related evaluations.
A health plan dependent of a current or former Briggs employee	(1) name; (2) Social Security number; (3) address; (4) dates related to you, such as date of birth; (5) telephone number; (6) email address; (7) account number; and (8) medical information and health insurance information, including health plan beneficiary number.