MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Jeffrey J. Boogay
Office: (267) 930-4784
Fax: (267) 930-4771
Email: jboogay@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

February 5, 2021

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 Greenworks Tools ("Greenworks") located at 500 South Main Street, Suite 450, Mooresville, North Carolina, 28115, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Greenworks 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 or about September 8, 2020, Greenworks learned of suspicious cyber activity affecting its online e-commerce website, www.greenworkstools.com. Greenworks immediately began working with third-party forensic investigators to determine what happened and whether any information was impacted. Greenworks also implemented additional procedures to further protect the security of customer debit and credit card information on its website.

The forensic investigators confirmed that www.greenworkstools.com was affected by a cyber-attack that may have compromised some payment card information entered on the website between September 3, 2020, and September 8, 2020. The source of the attack was the network of Guidance Solutions, Inc. ("Guidance"), a third-party web developer which Greenworks had retained to build and support its e-commerce website. On October 28, 2020, Guidance confirmed to Greenworks that an unauthorized attacker had obtained a Guidance employee's credentials and used them to alter files on www.greenworkstools.com. On December 28, 2020, Greenworks' investigation identified the circumstances revealing which customers may have been affected. The information

that could have been subject to unauthorized access includes cardholder's name, address, credit card number, expiration date, and CVV.

Notice to New Hampshire Resident

On or about February 5, 2021, Greenworks provided written notice of this incident to all affected individuals, which includes one (1) New Hampshire resident. 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, Greenworks moved quickly to investigate and respond to the incident, assess the security of Greenworks e-commerce website, and notify potentially affected individuals. Greenworks' investigation located the code responsible for the credit card/debit card compromise and has since removed the code from its e-commerce website.

Additionally, Greenworks 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. Greenworks 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) 930-4784.

Very truly yours,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB:ncl
Enclosure

EXHIBIT A

greenworks

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

Greenworks Tools ("Greenworks") writes to inform you of a recent event that may impact the privacy of some of your payment information. We wanted to provide you with information about the event, our response, and steps you may wish to take to better protect against the possibility of identity theft and fraud.

What Happened? On or about September 8, 2020, Greenworks learned of suspicious cyber activity affecting its online e-commerce website, www.greenworkstools.com. Greenworks immediately began working with third-party forensic investigators to determine what happened and whether any information was impacted. Greenworks also implemented additional procedures to further protect the security of customer debit and credit card information on our website. You can safely and securely use your payment card on our website.

The forensic investigators confirmed that www.greenworkstools.com was affected by a cyber-attack that may have compromised some payment card information entered on the website between September 3, 2020, and September 8, 2020. The source of the attack was the network of Guidance Solutions, Inc. ("Guidance"), a third-party web developer which Greenworks had retained to build and support its e-commerce website. On October 28, 2020, Guidance confirmed to Greenworks that an unauthorized attacker had obtained a Guidance employee's credentials and used them to alter files on www.greenworkstools.com.

Greenworks has taken steps to confirm the identity of the customers whose personally identifiable information might have been impacted by the cybersecurity incident. On December 28, 2020, our investigation identified the circumstances revealing which customers may have been affected. If you entered your payment card information on www.greenworkstools.com between September 3, 2020, and September 8, 2020, and then were redirected to a replica third-party checkout page that prompted you to re-enter your payment information, then your payment card information may have been impacted.

What Information Was Involved? Credit or debit card data from some credit and debit cards used on www.greenworkstools.com between September 3, 2020, and September 8, 2020, were impacted by this event. The specific information at risk because of this cybersecurity incident includes the cardholder's name, address, credit card number, expiration date, and CVV.

What We Are Doing. We take this incident and the security of your information seriously. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure payment information. In addition to notifying potentially impacted individuals we also notified state regulators, as required.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Help Protect Your Information.*

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call us at 888-490-0135, 9:00 a.m. to 9:00 p.m. Eastern Time, Monday through Friday, excluding U.S. holidays.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

Greenworks Tools

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Monitor Accounts

In general, 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 may 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 (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.

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 (7) 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); 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.

For Maryland residents, the Attorney General can be contacted by mail at 200 St. Paul Place, Baltimore, MD, 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov. ***For 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 violators. 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. We encourage you to 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. ***For 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/. ***For North Carolina residents,*** The North Carolina Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400, and online at www.ncdoj.gov.