STITES & HARBISON PLLC
ATTORNEYS

400 West Market Street
Suite 1800
Louisville, KY 40202-3352
(502) 587-3400
(502) 587-6391 FAX

Sarah Cronan Spurlock
(502) 681-0461
sspurlock@stites.com

January 7, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Dear Sir or Madam:

We represent Brinly-Hardy Co. ("BHC"), a company located in Jeffersonville, Indiana that manufactures and sells lawn and garden equipment. In compliance with Md. Code Ann. Com. Law § 14-3504, I am writing on BHC's behalf to notify your office of a cybersecurity incident that may have impacted personal information of two (2) Maryland residents.

Nature of the Incident

On November 18, 2021, BHC became aware of suspicious activity on its network when IT received a report that certain software was not working as expected. BHC began investigating immediately and determined that an unauthorized individual or individuals accessed one of its servers in the early morning of November 18, 2021 and began encrypting files using malicious software that impacted a number of servers and workstations. BHC's IT department detected the source of the attack and immediately disabled the account utilized, stopping the attack and preventing the infection from spreading. Through its investigation, BHC learned that the cyber criminals stole some data from its network during the attack. Because BHC detected and stopped the attack while it was occurring, it was able to prevent greater data theft but estimates the amount of data stolen to be roughly 5% of the company's data. Because BHC is unable to determine which portion of its data was stolen, BHC required time review the records of the impacted servers and workstations to identify individuals who may have had personal information exposed in the attack.

Personal Information Involved

The personal information that may have been compromised in this incident for two Maryland residents includes name, Social Security number, and health plan member number.

VIA E-MAIL

Notice to Maryland Residents

On January 7, 2022, BHC will provide written notice of this incident to impacted individuals, including the two Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as **Exhibit A**.

Steps Taken and to be Taken

In response to this incident, BHC has taken steps to enhance its security and prevent a similar attack in the future. These steps include: decommissioning the account used in the attack, strengthening remote desktop access controls, deploying a new anti-virus solution and advanced alerting for incident detection and response across its network, and beginning implementation of next-generation firewall technology to increase its defenses against unauthorized intrusions.

In its notice, BHC is providing information about steps individuals can take to protect their information, including contact information for the national consumer reporting agencies and the Federal Trade Commission. BHC is providing a toll-free number for notified individuals to call with questions. Additionally, BHC is making 12 months of credit monitoring available to notified individuals at no cost to them as an additional precaution.

Please do not hesitate to contact me if you have any questions regarding this notice.

Sincerely,

STITES & HARBISON PLLC

Sarah Cronan Spurlock

3230 Industrial Pkwy, Jeffersonville, IN 47130

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

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

On behalf of Brinly-Hardy Co., we are writing to notify you of the potential that some personal information about you may have been involved in a recent cyberattack on Brinly-Hardy Co. We take this incident seriously and we want you to be aware of what happened, the actions we are taking, and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

WHAT HAPPENED. On November 18, 2021, we became aware of suspicious activity on our network when IT received a report that certain software was not working as expected. We began investigating immediately and determined that an unauthorized individual or individuals accessed one of our servers in the early morning of November 18, 2021 and began encrypting files using malicious software that impacted a number of servers and workstations. Our IT department detected the source of the attack and immediately disabled the account utilized, stopping the attack and preventing the infection from spreading. Through our investigation, we learned that the cyber criminals stole some data from our network during the attack. Because we detected and stopped the attack while it was occurring, we were able to prevent greater data theft but estimate the amount of data stolen to be roughly 5% of our company data. Because we are unable to determine which portion of our data was stolen we have been working to review all of the records of the impacted servers and workstations to identify individuals who may have had personal information exposed in the attack. Once we confirmed the individuals who were potentially impacted, we began working with a cyber incident response vendor to provide you with this notice.

WHAT INFORMATION WAS INVOLVED. We cannot confirm that your personal information was actually accessed, viewed, or acquired during the attack. We are providing you this notification out of an abundance of caution because we cannot rule that possibility out. We have determined that the Brinly-Hardy Co. records that may have been impacted in the attack included certain reports and information we process in connection with our internal accounting and payroll, human resources, benefits, and business operations. The personal information about you involved in this incident may have included <<personal information>>.

WHAT WE ARE DOING. Brinly-Hardy Co. employs several security measures to safeguard our network and data. In response to this incident, we have taken additional steps to enhance our security and prevent a similar attack in the future, including: decommissioning the account used in the attack, strengthening remote desktop access controls, deploying a new anti-virus solution and advanced alerting for incident detection and response across our network, and beginning implementation of next-generation firewall technology to increase our defenses against unauthorized intrusions.

WHAT YOU CAN DO. Although we cannot confirm that the data stolen from us actually contained personal information, and we have no information that the data stolen from us has been fraudulently misused, we arranged to provide you with credit monitoring for 1 year at no cost to you as an added precaution. Brinly-Hardy Co. will cover the cost of this credit monitoring; however, you will need to enroll yourself in the credit monitoring if you wish to take advantage of this resource. Please review the instructions contained in the enclosed documents for information on steps you can take to protect your information, including detailed instructions on how to enroll in credit monitoring if you choose to do so.

FOR MORE INFORMATION. We sincerely regret any inconvenience this incident may cause you. We recognize that you may have questions not addressed in this letter. If you have additional questions, please contact our toll-free assistance line at 855-604-1719, Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely,

Jane Hardy
President & CEO, Brinly-Hardy Co.

Steps You Can Take to Protect Your Information

Enroll in Credit Monitoring.
As an added precaution, we have arranged to have TransUnion provide you with credit monitoring for 12 months at no cost to you. Please see the enclosed instructions if you wish to receive these credit monitoring services using the activation code provided.

Monitor Your Accounts.
Steps to protect against the possibility of identity theft or other financial loss include remaining vigilant for suspicious activity, reviewing your financial and other account statements, and monitoring your credit reports for suspicious activity.

Credit Reports. 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.

Security Freeze or Fraud Alert. 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 permission. 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. You cannot be charged to place, lift, or remove 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	**TransUnion**	**Equifax**
PO Box 9554	**PO Box 160**	**PO Box 105788**
Allen, TX 75013	**Woodlyn, PA 19094**	**Atlanta, GA 30348**
1-888-397-3742	**1-888-909-8872**	**1-800-685-1111**
www.experian.com/freeze/center.html	**www.transunion.com/credit-freeze**	**www.equifax.com/personal/credit-report-services**

If you request a security freeze with the above consumer reporting agencies, 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 years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military information, etc.)

You must follow the credit bureau's instructions to remove a security freeze. You may be required to send a written request to each of the three credit bureaus by mail and include proper identification (such as name, address, and social security number) and the PIN number 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.

As an alternative to a security freeze, you have the right to place a "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. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian
P.O. Box 2002
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, and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; www.ftc.gov/idtheft; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC. You can also further educate yourself about placing a fraud alert or security freeze on your credit file by contacting the FTC or your state's Attorney General. This notice was not delayed by a law enforcement investigation. ***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 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.

TransUnion

Activation Code: **<<Activation Code>>**

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a precaution, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<12 months>> provided by TransUnion Interactive, asubsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your creditmonitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422.** When prompted, enter the following 6-digit telephone pass code **<< Insertstatic 6-digit Telephone Pass Code >>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<12 months>> of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit reportonline, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online Credit Monitoring service anytime between now and **<<Insert Date>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, oran address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.