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

December 21, 2020

VIA FIRST-CLASS 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 Colony Hardware located at 269 S. Lambert Road Orange, CT 06477, and are writing to notify your office of an incident that may affect the security of some personal information relating to four (4) New Hampshire residents. 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, Colony Hardware 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

In March 2020, Colony Hardware discovered unusual activity on its network and immediately commenced an investigation to determine the nature and scope of the activity and to confirm the security of its network. This investigation of Colony Hardware's network, which included working with third-party forensic computer specialists, determined that Colony Hardware's network had been infected with malware that encrypted certain systems and disrupted company operations. The investigation confirmed that Colony Hardware's network had been subject to unauthorized access on March 3, 2020, at which time an unauthorized actor encrypted certain systems on the network. The investigation also determined that certain documents stored within Colony Hardware's environment could have been subject to unauthorized access or acquisition during that brief period.

Colony Hardware immediately began a comprehensive and lengthy review of the network locations identified by the investigation to identify any documents that may have been subject to unauthorized access and the information present in these locations during the brief period of unauthorized activity. After conducting a thorough review of its network, Colony Hardware confirmed the documents stored on its network that may have been accessible during the period of unauthorized access. While Colony Hardware was not able to confirm the extent to which documents in these locations were subject to unauthorized

access or acquisition and has no evidence of any misuse of any of information on these documents, it was unable to rule out the possibility of such access. Therefore, Colony Hardware undertook a lengthy and labor-intensive review of the items to determine what information was present at the time of the unauthorized activity. On September 21, 2020 Colony Hardware completed this review and determined the individuals who had personal information contained in the impacted documents. Colony Hardware continued to review its records to identify address information for these impacted individuals so they could be notified of the incident. After identifying address information for these individuals, Colony Hardware confirmed this population included four (4) New Hampshire residents. While the specific information that could have been subject to unauthorized acquisition varies by individual, it includes name, address, and Social Security number.

Notice to New Hampshire Residents

On or about December 21, 2020, Colony Hardware provided written notice of this incident to all affected individuals, which includes four (4) 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, Colony Hardware moved quickly to investigate and respond to the incident, assess the security of Colony Hardware systems, and notify potentially affected individuals. Colony Hardware is also working to implement additional safeguards and training to its employees and notified law enforcement of this incident. Colony Hardware is providing access to credit monitoring services for 24 months, through Experian, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Colony Hardware 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. Colony Hardware 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/ken

Exhibit A

COLONY

TOOLS & EQUIPMENT • SUPPLIES • SAFETY PRODUCTS • TOOL REPAIR • RENTALS

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

December 21, 2020

G0676-L01-0000001 T00017 P003 *********ALL FOR AADC 123
SAMPLE A SAMPLE - L01 GENERAL
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Dear Sample A Sample:

Colony Hardware writes to notify you of a recent incident that may affect the privacy of some of your personal information. *While we have no evidence of actual or attempted misuse of your information as a result of this incident*, this letter provides details about the incident, our response, and resources available to you to help protect your information should you feel it appropriate to do so.

In March 2020, Colony Hardware discovered unusual activity on its network and immediately commenced an investigation to determine the nature and scope of the activity and to confirm the security of its network. This investigation of Colony Hardware's network, which included working with third-party forensic computer specialists, determined that Colony Hardware's network had been infected with malware that encrypted certain systems and disrupted company operations. The investigation confirmed that Colony Hardware's network had been subject to unauthorized access on March 3, 2020, at which time an unauthorized actor encrypted certain systems on the network. The investigation also determined that certain documents stored within Colony Hardware's environment could have been subject to unauthorized access or acquisition during that brief period.

Colony Hardware immediately began a comprehensive review of the network locations identified by the investigation to identify any documents that may have been subject to unauthorized access and the information present in these locations during the brief period of unauthorized activity. After conducting a thorough review of its network, Colony Hardware confirmed the exact documents stored on Colony Hardware's network that may have been accessible during the period of unauthorized access. While Colony Hardware was not able to confirm the extent to which documents in these locations were subject to unauthorized access or acquisition, it was unable to rule out the possibility of such access. Therefore, Colony Hardware undertook a lengthy and labor-intensive review of the items to determine what information was present at the time of the unauthorized activity. On September 21, 2020, we completed this review and determined your information could have been subject to unauthorized access. Colony Hardware then worked to confirm address information for the notice population to provide notice soon thereafter.

What Information Was Involved? Our investigation determined your [Extra1], and name were present in the relevant documents and may have been accessible to an unauthorized actor for a limited period of time. Again, we are unaware of any actual or attempted misuse of your information.

What We Are Doing. The privacy and security of information are among our highest priorities and we have strict security measures in place to protect information in our care. Upon learning of unusual activity, we moved quickly to investigate and to respond to this incident and to confirm the security of our entire environment. Our response included taking steps to further secure our environment, working with third-party forensic computer specialists, and reviewing the impacted documents to determine whether and what personal information was present and could have been subject to unauthorized access. As part of our ongoing commitment to information security, we are also reviewing and enhancing existing policies and procedures related to data privacy.

Although we are unaware of any actual or attempted misuse of your personal information, we are offering you access to 24 months of credit monitoring and identity theft protection services through Experian at no cost to you as an added precaution. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Protect Your Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

What You Can Do. 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 and to detect errors. Please also review the information contained in the attached *Steps You Can Take to Protect Your Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If so, please contact our toll-free dedicated assistance line at (888) 994-0269 from 6:00 am - 8:00 pm PST, Monday through Friday and Saturday/Sunday from 8 am - 5 pm PST (excluding some U.S. national holidays). You may also write to Colony Hardware at 269 S. Lambert Road, Orange, CT 06477.

Sincerely,

COLONY HARDWARE

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **March 31, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: **https://www.experianidworks.com/credit**
- Provide your **activation code**: **ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 994-0269 by March 31, 2021. Be prepared to provide engagement number **DB24414** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 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.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents 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.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (888) 994-0269.

Monitor Accounts

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 listed below 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 160	P.O. Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
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

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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft prevention, 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.

For District of Columbia residents, the Attorney General for the District of Columbia may be contacted at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; (202) 727-3400; and https://oag.dc.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662; 1-888-743-0023; or www.oag.state.md.us. **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 Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000; or www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.