April 6, 2020

Sample A. Sample
123 Any Street
Apt. 1
Anytown, VT 01234

NOTICE OF DATA BREACH

Dear Sample A. Sample,

We are writing to inform you of a recent incident involving unauthorized access to some of our employees' email accounts. While we have no indication that your personal information has been misused, some of your information may have been in an email account that was accessed in this incident. We are writing to make you aware of our current understanding of what happened, measures that have been taken, and to provide you with some steps you can take to protect your personal information.

What happened?

On February 25, 2020, Spinrite, Inc. ("Spinrite") learned that an unauthorized party gained access to employee email accounts through a phishing attack. We immediately initiated an investigation and retained a leading computer security firm. During the course of the investigation, we learned that unauthorized connections were made to a limited number of Spinrite email accounts between November 29, 2019 and February 25, 2020. We were unable to confirm whether any specific emails or attachments stored within those affected accounts were viewed or acquired as a result of this incident. Out of an abundance of caution, we reviewed the emails stored in the affected email accounts to determine whether any of those emails contained personal information. We completed our review of the email accounts on March 23, 2020.

What information was involved?

We have determined that some of your personal information provided to Spinrite or to our affiliate Coats & Clark, Inc., was present in an affected email account, including some of the following information: first name, last name, [Extra1]. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

What we are doing.

As soon as we learned of this situation, we immediately launched an investigation and retained a leading computer security firm. We took steps to block unauthorized users from connecting to the affected email accounts, reset the relevant passwords, reviewed the contents of the documents in the email accounts to determine whether they contained personal information, and took additional measures to prevent unauthorized users from accessing employees' email accounts in the future. Based on our current investigation, we believe this incident was limited to the affected email accounts and did not impact our systems.

What you can do.

Although we do not have any evidence that your information has been misused, we recommend that you review the information provided in the enclosed "Further Information and Steps You Can Take." The

enclosure identifies some steps you can take to guard against the misuse of your personal information. Never provide personal information in a response to an electronic communication about a data security incident. Additionally, out of an abundance of caution, we are providing identity theft protection services through a one-year Experian IdentityWorks Membership at no cost to you. To activate this membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **June 30, 2020** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code**: **[Activation Code]**

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 [Toll-Free Number] by **June 30, 2020**. Be prepared to provide engagement number [Engagement Number] as proof of eligibility for the identity restoration services by Experian.

For more information.

We sincerely regret and apologize for any inconvenience this may cause you. Please do not hesitate to contact us at [Toll-Free Number] if you have any questions or concerns.

Sincerely,

Ryan Newell
President and CEO

Enclosure: Further Information and Steps You Can Take

Further Information and Steps You Can Take

Additional details regarding the One-Year 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 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 $1M Identity Theft Insurance**[2]: 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 [Toll-Free Number]. 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 (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 major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available for one 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.

Filing a Police Report for Suspicious Activity

We encourage you to remain vigilant of identity theft or fraud. You should review account statements, explanation of benefits, and credit reports and report any suspicious activity or suspected identity theft. You have the right to file a police report if you experience identity theft or fraud. If you do find suspicious activity of identity theft or fraud, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. In addition, you should report identity theft to your state's Attorney General and to the Federal Trade Commission ("FTC"). This notice has not been delayed by law enforcement.

Monitoring Your Accounts

You may obtain a free copy of your credit report from each of the credit bureaus once a year by visiting http://www.annualcreditreport.com, or calling 877-322-8228. Hearing impaired consumers can access TDD service at 877-730-4104. You may contact the nationwide credit bureaus at:

Equifax, 866-349-5191, P.O. Box 740241, Atlanta, GA 30374, www.equifax.com/FCRA.
Experian, 888-397-3742, P.O. Box 9701, Allen, TX 75013, www.experian.com.
TransUnion, 800-916-8800, P.O. Box 2000, Chester, PA 19022, www.transunion.com.

You may also place a fraud alert or security freeze on your credit report at no cost. A fraud alert is a notice that can be placed on a consumer's credit report that alerts companies who may extend credit that the consumer may have been a victim of identity theft or fraud. When a fraud alert is displayed on a consumer's credit file, a business is required to

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

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

take steps to verify the consumer's identity before extending new credit. There are two types of fraud alerts: an "initial" fraud alert that lasts for one year, and an "extended" fraud alert for victims of identity theft or fraud that lasts seven years. A fraud alert should not affect your ability to get a loan or credit, but it may cause some delay if you are applying for credit. To place a fraud alert, please contact one of the credit reporting agencies at:

Equifax, 888-836-6351, P.O. Box 105069, Atlanta, GA 30348, www.equifax.com/personal/credit-report-services.
Experian, 888-397-3742, P.O. Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html.
TransUnion, 800-680-7289, P.O. Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts.

Alternatively, you may place a security freeze on your file. Security freezes will prevent new credit from being opened in your name without the use of a personal identification number or password that will be issued by the credit reporting agencies after you initiate the freeze. In order to place a security freeze, you may be required to provide the credit reporting agencies with information that identifies you. A security freeze can make it more difficult for someone to get credit in your name, but it also may delay your ability to obtain credit. The credit reporting agencies may not charge a fee to place a freeze or remove a freeze. To place a security freeze, please contact one of the agencies at:

Equifax, 888-298-0045, P.O. Box 105788, Atlanta, GA 30348, www.equifax.com/personal/credit-report-services.
Experian, 888-397-3742, P.O. Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html.
TransUnion, 888-909-8872, P.O. Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze.

Additional Information
You may find additional information about fraud alerts, security freezes, and suggestions you can take to protect yourself from identity theft or fraud by contacting the FTC or your state Attorney General.

The FTC provides suggestions for actions you may take in the event of identity theft at www.consumer.ftc.gov/features/feature-0014-identity-theft. You may also call the FTC for more information at 1-877-ID-THEFT (438-4338) (TTY: 1-866-653-4261), or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

For California Residents: Visit the California Office of Privacy Protection (http://ww.ca.gov/Privacy) for additional information on protection against identity theft.

For Maryland Residents, you can find more information regarding steps to avoid identity theft from the Maryland Attorney General's Office: The Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.marylandattorneygeneral.gov.

For North Carolina Residents, the North Carolina Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For New Mexico Residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"), which include among other things, the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer bureaus correct or delete inaccurate, incomplete, or unverifiable information. For further information about the FCRA, visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

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; www.ag.ny.gov.

For Oregon Residents: You can report suspected identity theft to the Oregon Attorney General at (877) 877-9392, (503) 378-4400, Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, or at www.doj.state.or.us.

For Rhode Island Residents: The Rhode Island Attorney General provides information about identity theft at http://www.riag.ri.gov/homeboxes/Consumer.php. You may also contact the Consumer Protection Unit at (401) 274-4400, or by mail at 150 South Main Street, Providence RI 02903. At this time, we believe there are approximately 3 Rhode Island residents involved in this incident.