

# **EXHIBIT 1**

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Rock-It Global (“RIG”) located at 1002 Lititz Pike, Suite 238, Lititz, PA 17543, does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

### **Nature of the Data Event**

On or about March 7, 2023, RIG became aware of suspicious activity related to an employee’s computer. We immediately worked to secure our systems and launched an investigation, with assistance from third-party cybersecurity and forensic specialists, to determine the nature and scope of the incident. Through the investigation, it was determined that there was unauthorized access to certain RIG’s files stored on the employee’s computer from February 13, 2023, to March 7, 2023.

While RIG has not received any reports of fraudulent misuse of any information as a result of this incident, in an abundance of caution, RIG undertook a comprehensive and time-intensive review of the involved files to determine whether sensitive information was present in the involved files at the time of the incident. That process was completed. RIG then worked to identify contact information for the impacted individuals. The information that could have been subject to unauthorized access includes name and Social Security number.

### **Notice to Maine Residents**

On or about July 19, 2023, RIG provided written notice of this incident to three (3) Maine 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, RIG moved quickly to investigate and respond to the incident, assess the security of RIG systems, and identify potentially affected individuals. Further, RIG notified federal law enforcement regarding the event. RIG is also working to implement additional safeguards and training to its employees. RIG is providing access to credit monitoring services for two (2) years through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, RIG is providing impacted individuals with guidance on how to better protect against identity theft and fraud. RIG 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.

# **EXHIBIT A**



<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

<<b2b\_text\_1(NOTICE OF [SECURITY INCIDENT] / [DATA BREACH])>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Rock-It Global (“RIG”) is writing to inform you of an incident that may involve some of your information. Although there is no indication that your information has been misused in relation to this incident, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

**What Happened?** On or about March 7, 2023, RIG became aware of suspicious activity related to an employee’s computer. We immediately worked to secure our systems and launched an investigation, with assistance from third-party cybersecurity and forensic specialists, to determine the nature and scope of the incident. Through the investigation, it was determined that there was unauthorized access to certain RIG’s files stored on the employee’s computer from February 13, 2023, to March 7, 2023.

While we have not received any reports of fraudulent misuse of any information as a result of this incident, in an abundance of caution, RIG undertook a comprehensive and time-intensive review of the involved files to determine whether sensitive information was present in the involved files at the time of the incident. That process was recently completed. RIG then worked to identify contact information for the impacted individuals. We are notifying you because that investigation determined certain information related to you was present in the involved files.

**What Information Was Involved?** The information in the involved files includes your <<b2b\_text\_2(name, data elements)>><<b2b\_text\_3(data elements cont.)>>. To date, we have not received any reports of fraudulent misuse of any information as a result of this incident.

**What We Are Doing.** Data privacy and security are among our highest priorities, and we have security measures in place to protect information in our care. Upon learning of the activity, we immediately took steps to further secure our systems and investigate the incident. We will also notify applicable federal and state regulators, as necessary.

While we are unaware of any fraudulent misuse of your information as a result of this incident, as an added precaution, we are also offering 24 months of complimentary access to identity monitoring services through Kroll. Individuals who wish to receive these services must activate by following the attached instructions.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity over the next twelve (12) to twenty-four (24) months. You may also review the enclosed *Steps You Can Take to Help Protect Personal Information* to learn helpful tips to protect your information, should you feel it appropriate to do so. There you will find more information on the identity monitoring services we are making available to you. While RIG will cover the cost of these services, you will need to complete the activation process.

**For More Information.** We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our dedicated assistance line at [Rock-It TFN](#), 8:00 a.m. to 5:30 p.m., Central Time, excluding some U.S. holidays. You can also write to RIG at 1002 Lititz Pike, Suite 238, Lititz, PA 17543. We apologize for any inconvenience or concern this incident may cause.

Sincerely,

Rock-It Global

## STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

### Activate your Monitoring Services

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b\_text\_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s\_n>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).

Additional information describing your services is included with this letter.

### Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit 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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

## **Additional Information**

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; [www.identitytheft.gov](http://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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

*For District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

*For New Mexico residents*, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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 New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

*For Rhode Island residents*, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; [www.riag.ri.gov](http://www.riag.ri.gov); and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this incident. There are approximately [#] Rhode Island residents that may be impacted by this incident.

# **KROLL**

## **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.