EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Rockler does not waive any rights or defenses regarding the applicability of Washington law, the applicability of the Washington data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about May 13, 2022, Rockler discovered suspicious activity within its computer environment. Rockler acted fast and cut off access to the cyber attackers in less than 4 hours. With the assistance of forensic specialists, Rockler immediately launched an investigation to determine the nature and scope of the activity. The investigation identified that an unauthorized actor may have had access to Rockler's environment between May 13, 2022 and May 16, 2022. On or about May 18, 2022, the investigation determined that that unauthorized actor had access to certain files and folders within its system which represents less than 1% of the data on its system.

Although Rockler is unaware of any actual or attempted misuse of information at this time, Rockler engaged specialists to complete a manual and programmatic review of the accessible files and folders to determine whether sensitive information was present. This lengthy review of the data review team required months to complete. On January 10, 2023, the review was completed and Rockler determined that some sensitive information was present in the potentially accessed files. Out of an abundance of caution, Rockler is providing notice to all individuals who may have been impacted.

The information that could have been subject to unauthorized access includes name, and Social Security number, Date of Birth, Driver's License number, Passport number, Financial Account information, Payment card information, medical information and health insurance information.

Notice to Washington Residents

On or about February 17, 2023, Rockler provided written notice of this incident to approximately one thousand eight hundred thirty-seven (1,837) Washington 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, Rockler moved quickly to investigate and respond to the incident, assess the security of Rockler systems, and identify potentially affected individuals. Rockler implemented additional safeguards and training to its employees. Rockler is providing access to complimentary credit monitoring services through Experian, to those individuals with their Social Security number or financial account information potentially impacted.

Additionally, Rockler 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. Rockler 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.

Rockler is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

ROCKLER

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>>

NOTICE OF <<VARIABLE HEADER>>

Dear <<Name 1>>:

I am writing you on behalf of Rockler Companies, Inc. to inform you of a recent incident that may impact the privacy of some of your personal information. Although we are not aware of any actual or attempted misuse of your information at this time, we know it is our responsibility to provide you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so. At Rockler, our values require us to ensure we respect the privacy of your information and prioritizes the confidentiality and security of the information within our care. We spared no effort to make sure that we did everything we could to fight off the cyber-attack we experienced quickly, and are now reaching out to provide you with information and tools help you minimize the risk of identity theft and fraud.

What Happened? On or about May 13, 2022, Rockler discovered suspicious activity within its computer environment. Our team acted fast, and we cut off access to the cyber attackers in less than 4 hours. With the assistance of forensic specialists, we immediately launched an investigation to determine the nature and scope of the activity. The investigation identified that an unauthorized actor may have had access to our environment between May 13, 2022 and May 16, 2022. On or about May 18, 2022, the investigation determined that that unauthorized actor had access to certain files and folders within our system which represents less than 1% of the data on our system.

Although we are unaware of any actual or attempted misuse of your or any other information at this time, we engaged specialists to complete a manual and programmatic review of the accessible files and folders to determine whether sensitive information was present. This lengthy review of the data review team required months to complete. On January 10, 2023, the review was completed and we determined that you had some sensitive information present in the potentially accessed files. Out of an abundance of caution, we are providing notice to all individuals who may have been impacted.

What Information Was Involved? Our investigation determined the following information relating to you was present in files stored on our systems during the period of unauthorized access: name, <<Breached Elements>>. Please note, we have no evidence of any actual or attempted misuse of personal information as a result of this security incident.

What We Are Doing. We take this incident and the security of personal information in our care very seriously. In response to the security incident, we promptly took steps to secure the environment, including rotating passwords, and conducting a diligent investigation aided by third-party forensic specialists, to confirm the full nature and scope of the event. Further, as part of our ongoing commitment to the privacy of information in our care, we implemented additional technical security measures designed to mitigate recurrence of this type of incident. We also have created a process of continuous improvement to review and enhance our existing data privacy policies and procedures on an ongoing basis.

As an added precaution, we are also providing you with access to <<CM Length>> months of complimentary identity monitoring and restoration services through Experian, along with guidance on how to better protect against the possibility of information misuse. We are covering the cost of these services, but due to privacy restrictions, you will need to complete the activation process yourself using the enrollment instructions below.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanations of benefits, as applicable, and by monitoring your free credit reports for suspicious activity and to detect errors. You can find out more about how to protect against the potential misuse of information in the enclosed *Steps You Can Take to Protect Personal Information.* There, you will also find more information about the identity monitoring services we are offering and how to enroll.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. As a result, we have partnered with Epiq who specializes in handling this type of incident and can help you with any additional questions you have. Please call 877-516-6134, 9:00 AM – 9:00 PM Monday through Friday, excluding U.S. holidays. You may also write to us at: 4365 Willow Dr., Medina MN, 55340.

In our world, cyber threats have become a bigger and bigger risk to the security of everyone's personal information. At Rockler, we are committed to continue to enhance our security systems to help protect your information.

Sincerely,

Steven Singer
CEO
Rockler Companies, Inc.

Steps You Can Take to Protect Personal Information

Enroll in Credit Monitoring

To help protect your identity, we are offering a complimentary <<CM Length>>-month 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**: **<<Enrollment Deadline>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- 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 877.288.8057 by **<<Enrollment Deadline>>.** Be prepared to provide engagement number **<<Engagement Number>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR <<CM LENGTH>>**-MONTH 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, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists 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.

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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 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 your name without your consent. However, you should be aware that using a credit 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 credit freeze on your credit report. To request a security freeze, you will need to provide 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 you are a victim of identity theft.

---

* Offline members will be eligible to call for additional reports quarterly after enrolling

** 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.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	**Experian**	**TransUnion**
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
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

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and 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 www.oag.state.md.us.

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 bureaus 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 violator. 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 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.