

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

JASON MICHAEL GOODWIN
jgoodwin@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, Pennsylvania 19422

Visit us online at
www.C-WLAW.com

Telephone: (610) 567-0700
Fax: (610) 567-0712

February 8, 2023

Via Email

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202
Idtheft@oag.state.md.us

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Sonder Holdings Inc. (“Sonder”) with mailing address at 500 E 84th Ave., Suite A-10, Thornton, CO, 80229 and provide this notification to your Office of a recent data security incident. Sonder is a tech-enabled hospitality company, providing hotel and professionally managed and serviced apartment accommodations in North America, Europe, and the Middle East. By providing this notice, Sonder does not waive any rights or defenses under Maryland law, including the data breach notification statute.

After receiving an unsolicited email from an unknown threat actor on November 13, 2022 alleging access to certain Sonder information, Sonder immediately commenced an investigation and confirmed, on November 14, 2022, that one of its Amazon Web Services (“AWS”) accounts had been subject to unauthorized access (the “Incident”). Sonder took immediate action to address and investigate the Incident, [REDACTED]

[REDACTED] Additionally, while Sonder’s investigation was ongoing, Sonder provided public notification of this Incident on November 23, 2022 via press release and a posting on the Sonder blog website, where news and information relating to Sonder is typically posted.

The investigation commenced by Sonder determined that the unknown threat actor utilized one access credential acquired through unknown means to access one of Sonder’s AWS accounts. Based on the investigation, the initial access to the AWS account by the threat actor appears to have been on May 21, 2022. The threat actor accessed the AWS account a limited number of times thereafter, the last access taking place on November 14, 2022. As part of the investigation, a thorough review of Sonder’s AWS environment was performed with the assistance of outside specialists engaged by Sonder via outside counsel to determine the types of information contained within the various datasets stored in the accessed AWS account, [REDACTED]

[REDACTED] This review ultimately determined that the personal information, as defined under your jurisdiction’s data breach notification law, of approximately 108 individuals in your state was accessible to the threat actor.

Sonder is providing notice of this Incident to potentially impacted individuals, including the 108 individuals in your state referenced above, on February 8, 2023. The notice letter includes an offer of complimentary credit monitoring and identity protection services offered through Kroll for twelve (12) months. The notice letter being sent to individuals is substantially similar to the letter attached hereto as ***Exhibit A***.

Please contact me should you have any questions.

Very truly yours,

CIPRIANI & WERNER, P.C.

By: 
Jason M. Goodwin

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 DATA BREACH)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing to inform you of a data security incident experienced by our company that may have involved your information as described below. We take the privacy and security of all information very seriously and are providing information about the incident and steps you can take to help protect your information.

What Happened: After receiving an unsolicited email from an unknown threat actor, on November 13, 2022, alleging access to certain Sonder information, we immediately commenced an investigation and confirmed, on November 14, 2022, that one of our Amazon Web Services (AWS) accounts had been subject to unauthorized access. Upon discovery, we took action to address and investigate the incident, as described further below. Based on our investigation, the initial access by the threat actor appears to have occurred on May 21, 2022, with the last access on November 14, 2022, the date Sonder confirmed the access and disabled the access credential used by the threat actor.

What Information Was Involved: The information that may have been accessible to the threat actor includes first and last name, address, email address, phone number, date of birth, government-issued photo identification, last four digits of credit card number, username, guest transaction receipts, IP address, and dates booked for past stays at Sonder properties.

What We Are Doing: Upon learning of this incident, we immediately took steps to address the incident, including disabling the threat actor's access to the AWS account at issue, engaging outside counsel and leading security and forensic specialists to assist with determining the nature and scope of the incident, and notifying law enforcement. Additionally, we are offering you complimentary identity monitoring services for 12 months through Kroll in an abundance of caution. Kroll has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. Due to privacy laws, we cannot register you directly. Activating these services will not affect your credit score. You can find activation instructions below.

What You Can Do: We recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, as well as identity monitoring activation instructions.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line, which can be reached at sonder@krollsupport.com or 1-855-504-2761, from 8:00 a.m. to 5:30 p.m. Central Time, Monday through Friday, excluding major U.S. holidays. If you are calling from outside of the U.S., Canada, or Mexico, you may reach our dedicated international assistance line at any time at +44 20 7570 0344. Additional information may also be found at sonderinfo.kroll.com. Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

Phil Rothenberg, General Counsel

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity Monitoring Services

Visit [<<IDMonitoringURL>>](IDMonitoringURL) to activate and take advantage of your identity monitoring services.

You have until [<<b2b_text_6 \(activation date\)>>](b2b_text_6 (activation date)) to activate your identity monitoring services.

Membership Number: [<<Membership Number s_n>>](Membership Number s_n)



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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.

Monitor Your Accounts and Credit Reports

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, 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 lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your 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 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 credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); 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.

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

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

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, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. Sonder may be contacted at 500 E 84th Ave., Suite A-10, Thornton, CO, 80229, United States, Attn: General Counsel.

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 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.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 14 Rhode Island residents impacted by this incident.

For Washington, D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>. Sonder may be contacted at 500 E 84th Ave., Suite A-10, Thornton, CO, 80229, United States, Attn: General Counsel.