

May 8, 2023

Via Certified Mail; Return Receipt Requested:

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Cybersecurity Incident Involving Procurri, LLC

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Procurri, LLC ("Procurri"), a data center equipment and lifecycle services provider located at 5825 Peachtree Corners East, Suite A, Norcross, GA 30092, with respect to a recent cybersecurity incident that was first discovered by Procurri on April 10, 2023 (hereinafter, the "Incident"). Procurri takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of residents being notified, and the steps that Procurri has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On April 10, 2023, Procurri Europe Lifecycle Services, Ltd. detected unusual activity on their network, which extended to the Procurri, LLC network. Upon discovery of this incident, Procurri, LLC immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. At the time of writing, the forensic investigation is currently ongoing, and there is no evidence that suggests any sensitive personal information was fraudulently misused or acquired. The identity of the person responsible for the unauthorized activity remains unknown.

Although Procurri is unaware of any fraudulent misuse or acquisition of information, it is possible that individuals' may have been exposed as a result of this unauthorized activity.

As of this writing, Procurri has not received any reports of related identity theft since the date of the incident (April 10, 2023 to present).

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com



2. Number of New Hampshire residents affected.

A total of two (2) New Hampshire residents may have been potentially affected by this incident. Notification letters to these individuals were mailed on May 5, 2023 and May 8, 2023, by electronic mail and first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Procurri is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, Procurri moved quickly to investigate and respond to the Incident, assessed the security of its systems, and notified the potentially affected individuals out of an abundance of caution. Specifically, Procurri, LLC immediately disconnected all access to the network, engaged a specialized third-party cybersecurity firm, engaged counsel, notified the Federal Bureau of Investigation, and notified the requisite government authorities in the United States. Procurri is taking other various steps to remediate vulnerabilities in their systems such as deploying an end point detection software monitored 24 hours a day, 7 days a week. As the forensic investigation continues, Procurri will implement additional security measures as deemed necessary.

Although Procurri is not aware of any actual or attempted misuse of the affected personal information, Procurri offered eighteen (18) months of complimentary credit monitoring and identity theft restoration services through IDShield to all individuals to help protect their identity. Additionally, Procurri provided guidance on how to better protect against identity theft and fraud, including providing 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 the contact details for the Federal Trade Commission.

4. Contact information

Procurri remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

**Procurri LLC**

A Subsidiary of Procurri Corporation Pte. Ltd.

5825 Peachtree Corners East
Suite A, Norcross
GA 30092, USA

May 8, 2023

RE: Notice of Data Security Incident

Please read this entire letter.

Dear [REDACTED]

Procurri, LLC is contacting you regarding a recent data security incident that occurred on April 10, 2023, that may have resulted in an unauthorized access to your sensitive personal information. While we are unaware of any fraudulent misuse or acquisition of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened?

On April 10, 2023, Procurri Europe Lifecycle Services, Ltd. detected unusual activity on their network, which extended to the Procurri, LLC network. Upon discovery of this incident, Procurri, LLC immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm to assist with securing the environment, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. At the time of writing, the forensic investigation is currently ongoing, and there is no evidence that suggests any of your sensitive personal information was fraudulently misused or acquired.

What Information Was Involved?

Although Procurri, LLC has no evidence that any sensitive information has been misused or acquired by third parties as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the currently ongoing investigation, the following information related to you may have been subject to unauthorized access: [REDACTED]

What We Are Doing to Protect Your Information:

Data privacy and security is among Procurri, LLC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Since the discovery of the incident, Procurri, LLC moved quickly to investigate, respond, and confirm the security of our systems. Specifically, Procurri, LLC immediately disconnected all access to the network, engaged a specialized third-party cybersecurity firm, engaged counsel, notified the Federal Bureau of Investigation, and notified the requisite government authorities in the United States. We are taking other various steps to remediate vulnerabilities in our systems such as deploying an end point detection software monitored 24 hours a day, 7 days a week. As the forensic investigation continues, we will implement additional security measures as deemed necessary.



Procurri LLC
A Subsidiary of Procurri Corporation Pte. Ltd.

5825 Peachtree Corners East
Suite A, Norcross
GA 30092, USA

As a precautionary measure, to help protect your identity, we are also offering a complimentary 18-month membership with IDShield.

IDShield provides comprehensive Identity and credit monitoring, real-time alerts and direct access to dedicated licensed private investigators who will restore your identity if stolen. This product provides you with Identity detection and resolution of identity theft.

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 or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the credit monitoring services we are making available to you at no cost. To activate your membership and start monitoring your personal information please follow the steps below:

- Enroll by June 8th, 2023.
- Enrollment Portal

- [REDACTED]
- [REDACTED]
- [REDACTED]

IDShield Plan Benefits Include:

- Identity Consultation and Advice
- Online Privacy and Reputation Management
- Financial Account Protection
- \$1 Million Identity Fraud Protection Plan
- Child Monitoring (Family plan only)
- Identity and Credit Monitoring
- Identity and Credit Threat Alerts
- Full-Service Identity Restoration
- Direct Access to Licensed Private Investigators
- Monthly Credit Score Tracker
- Social Media Monitoring
- Mobile App
- **Customer Care**
 - Customer Care is available from 7:00am to 7:00pm CST to answer any questions regarding the IDShield plan, assist with enrollment or activation of their IDShield memberships. I have listed their contact information below.
 - PPLSI Customer Care
[REDACTED]
Monday-Friday
7am to 7pm CST



Procurri LLC

A Subsidiary of Procurri Corporation Pte. Ltd.

5825 Peachtree Corners East
Suite A, Norcross
GA 30092, USA

Please note that this credit and identity monitoring is available to you free of charge for 18 months from the date of this letter once you enroll in the program. The program covers you as the employee of Procurri and if you were enrolled in full family coverage with our medical benefits you can elect to cover your family within this program.

We would like to reiterate that, at this time, there is no evidence that your information was misused or acquired. However, we encourage you to take full advantage of the services offered.

For More Information

Should you have any questions or concerns regarding this matter, please do not hesitate to contact the Human Resources Department at [REDACTED]

Sincerely,

Kristie Jeng
Head of Human Resources – Americas
on behalf of and for Procurri, LLC

**Procurre LLC**

A Subsidiary of Procurre Corporation Pte. Ltd.

5825 Peachtree Corners East
Suite A, Norcross
GA 30092, USA**Steps You Can Take to Help Protect Your Information**

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

ExperianP.O. Box 9554
Allen, TX 75013
1-888-397-3742www.experian.com/fraud/center.html**TransUnion**P.O. Box 2000
Chester, PA 19016
1-800-680-7289www.transunion.com/fraud-alerts**Equifax**P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

Security Freeze: You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

ExperianP.O. Box 9554
Allen, TX 75013
1-888-397-3742www.experian.com/freeze/center.html**TransUnion**P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872www.transunion.com/credit-freeze**Equifax**P.O. Box 105788
Atlanta, GA 30348-5788
1-888-298-0045<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, 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: Changing The Way The World Buys Technology procurre.com



Procurri LLC
A Subsidiary of Procurri Corporation Pte. Ltd.

5825 Peachtree Corners East
Suite A, Norcross
GA 30092, USA

600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. Instances of known or suspected identity theft should also be reported to law enforcement.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For residents of New Mexico: State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 agencies 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 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 at 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 residents of Oregon: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island: You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov

District of Columbia Office of the Attorney General - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois office of the Attorney General - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us

New York Office of Attorney General - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

North Carolina Office of the Attorney General - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; www.ncdoj.com

Rhode Island Office of the Attorney General - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; www.riag.ri.gov