EXHIBIT 1

We represent Young Consulting LLC ("Young Consulting") located at 3200 Windy Hill Road SE, Suite 1400W, Atlanta, GA 30339, and are writing to notify your office on behalf of Blue Shield of California ("Blue Shield") and/or other covered entities, of an incident that may affect the security of certain personal information relating to eight hundred forty-seven (847) Maine residents. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Young Consulting and the covered entities do 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 April 13, 2024, Young Consulting became aware of technical difficulties in their computer environment. Young Consulting immediately took certain systems offline to contain the incident and launched an investigation, with the assistance of a cybersecurity forensics firm, to determine the nature and scope of the event. The investigation determined that an unauthorized actor gained access to Young Consulting's network between April 10, 2024, and April 13, 2024, and downloaded copies of certain files.

During the review process, Young Consulting worked to determine what information was contained within the involved files, and to identify the individuals whose information may have been involved. That process is ongoing, however, during this process, Young Consulting identified that information relating to certain data owners, including Blue Shield and the above referenced covered entities, may have been impacted and provided those data owners with copies of the potentially impacted files. On June 28, 2024, Young Consulting provided confirmation to Blue Shield that those files were accessed by an unauthorized actor. Young Consulting then worked to identify appropriate contact information for the impacted individuals to begin providing notification.

The information involved varies by individual but may include name, Social Security number, date of birth, insurance policy/claim information, prescriptions, and provider name.

Notice to Maine Residents

On August 26, 2024, Young Consulting began providing written notice of this incident to eight hundred forty-seven (847) 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 learning of the event, Young Consulting took immediate steps to secure its environment, investigate the activity, and notify federal law enforcement. As part of its ongoing commitment to the privacy of information in its care, Young Consulting is reviewing its policies, procedures, and processes related to the storage and access of sensitive information to prevent a similar incident from occurring in the future. Young Consulting is providing access to credit monitoring services for one (1) year through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Young Consulting is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to monitor their free credit reports and Explanations of Benefits. Young Consulting 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.

Young Consulting 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. Young Consulting is also notifying the U.S. Department of Health and Human Services and prominent media outlets pursuant to the Health Insurance Portability and Accountability Act (HIPAA).

EXHIBIT A

Young Consulting
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

YOUNG CONSULTING

August 26, 2024

NOTICE OF DATA BREACH

Dear

Young Consulting, LLC ("Young Consulting") is writing to inform you of a recent incident. Young Consulting provides risk management services to Blue Shield of California ("Blue Shield") and receives information from Blue Shield relating to these services. While we are unaware of any actual misuse of your information at this time, we are providing you with this notice out of an abundance of caution, to inform you of the incident, our response, and steps you may take to help protect your information, should you feel it necessary to do so.

What Happened? On April 13, 2024, Young Consulting became aware of technical difficulties in our computer environment. We immediately took certain systems offline to contain the incident and launched an investigation, with the assistance of a cybersecurity forensics firm, to determine the nature and scope of the event. The investigation determined that an unauthorized actor gained access to Young Consulting's network between April 10, 2024, and April 13, 2024, and downloaded copies of certain files.

During our review process, we worked to determine what information was contained within the involved files, and to identify the individuals whose information may have been involved. That process was recently completed and Young Consulting provided Blue Shield with copies of the files potentially impacted. On June 28, 2024, Young Consulting provided confirmation to Blue Shield that those files were accessed by an unauthorized actor. We then worked to identify appropriate contact information for the potentially impacted individuals so that we could provide notification.

What Information Was Involved? Your information that may have been accessed or acquired includes your name, Social Security number, date of birth, and insurance claim information.

What We Are Doing. Young Consulting takes this incident very seriously, and we are committed to maintaining your privacy. Upon learning of the incident, we took immediate steps to secure our computer environment, investigate the activity, and notify law enforcement. As part of our ongoing commitment to the privacy of information in our care, we are reviewing our policies, procedures, and processes related to the storage and access of sensitive information to prevent something like this from happening in the future.

As an added precaution we are offering you access to 12 months of complimentary credit monitoring services through Cyberscout, a TransUnion company. Individuals who wish to receive these services must enroll by following the below enrollment instructions, as we are unable to activate them on your behalf.

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 and to detect errors. You can also review the enclosed *Steps You Can Take to Protect Personal Information*. There you will find information on how to enroll in the complimentary credit monitoring services we are offering to you.

For More Information. We understand that 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 1-833-448-2610, toll-free between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. You may also write to us at: Young Consulting, LLC, 3200 Windy Hill Road SE, Suite 1400W, Atlanta, GA 30339.

Sincerely,

Young Consulting, LLC

Steps You Can Take To Protect Personal Information

Enroll in Monitoring Services

In response to the incident, we are providing you with access to Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **www.mytrueidentity.com** and follow the instructions provided. When prompted please provide the following unique code to receive services: . In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

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 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:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
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; 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; 1-202-442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 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, 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.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 592 Rhode Island residents that may be impacted by this event.