EXHIBIT 1

This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Open Practice Solutions, LTD ("OPS") 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 June 26, 2025, OPS was alerted to a potential issue in the billing summary available within its billing portal. OPS immediately launched an investigation and determined that due to a misconfiguration in a software update deployed that morning, portal users were able to view the billing summary of certain other users affiliated with the same provider. This misconfiguration was in place for approximately five (5) hours. OPS then undertook a comprehensive review of the at-risk data to determine if any sensitive information could be affected, and to whom it related. Once its investigation was complete, OPS began notifying impacted customers on August 20, 2025, with the offer to provide notice to individuals and regulators on those customers' behalf.

The information that could have been subject to unauthorized access includes individual's first and last name, provider name, date of service, and service provided. Addresses, phone numbers, Social Security numbers, financial account information and health insurance information were not viewable and were not involved in this error.

Since the event, OPS has implemented new security enhancements to better protect user information that include:

1. **Enhanced Data Filtering**: These filters ensure that the data sent to a user's browser belongs to them, preventing the possibility of cross-account data exposure. If an error occurs, the user will be logged out and a high priority alert is sent to OPS.
2. **Enhanced Development Processes**: OPS further matured its Software Development Life Cycle by refining processes, retraining teams, and embedding stronger security protocols. This ensures that security is central at every stage of software design and deployment, while positioning OPS to evolve with best practices and emerging standards.
3. **Expanded Automated Testing**: OPS added more automated tests to its software build procedures. This creates an additional layer of security to automatically catch potential configuration issues before any system updates are released.

Notice to Washington Residents

On October 10, 2025, OPS began providing written notice of this incident to one thousand two hundred two (1,202) 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, OPS moved quickly to investigate and respond to the incident, assess the security of OPS systems, and identify potentially affected individuals.

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

OPS is providing written notice of this incident to relevant state and federal regulators, as necessary, including the U.S. Department of Health and Human Services and prominent media pursuant to Health Insurance Portability and Accountability Act (HIPAA), and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

EXHIBIT A

Open Practice Solutions
300 Executive Pkwy W STE 300
Hudson, OH 44236

RETURN SERVICE REQUESTED

Dear ,

We are writing to notify you of an error that may have involved some of your information. OPS is providing information about the error, 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 June 26, 2025, we were alerted to a potential issue in the billing summary available within our billing portal. We immediately launched an investigation and determined that due to a misconfiguration in a software update deployed that morning, another OPS customer may have had access to some of your billing information. This misconfiguration was in place for approximately five (5) hours. Although we have no evidence that your information was specifically viewed, we are providing this notification out of an abundance of caution. We are not aware of any attempted misuse of your information.

What Information Was Involved? The information potentially involved included your first and last name, provider name, date of service and service provided. Your address, phone number, Social Security number, financial account information and health insurance information were **NOT** viewable and were **NOT** involved in this error.

What We Are Doing. The confidentiality, privacy, and security of personal information is among our highest priorities, and we have strict security measures in place to protect information in our care. Upon becoming aware of this error, we immediately took steps to correct the misconfiguration and conducted an investigation to determine the full scope of potentially accessed information.

What You Can Do. While we do not believe you need to take any specific action as a result of this error, we are providing the enclosed "Steps You Can Take to Help Protect Personal Information" as a guide to general best practices.

For More Information. We understand that you may have questions about this error that are not addressed in this letter. If you have additional questions or need assistance, please call our dedicated assistance line at **877-396-3218** between the hours of 9:00 a.m. to 9:00 p.m. Eastern time, Monday through Friday, excluding all major U.S. holidays.

Sincerely,

Open Practice Solutions

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

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/data-breach-help
1-888-298-0045	1-888-397-3742	1-833-799-5355
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion, 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, 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 their 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; (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; 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 event. There are approximately 54 Rhode Island residents that may be impacted by this event.