EXHIBIT 1

We continue to represent Quality Behavioral Health ("QBH") located at 900 7th St, Clarkston, WA 99403, and write to supplement our previous notice to your office dated December 26, 2022. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, QBH 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 November 26, 2022, QBH learned that it experienced a cyber incident. It promptly took steps to secure its systems and commenced an investigation into the nature and scope of the incident. QBH has been working diligently to investigate the incident and confirm any information that may be affected. While the investigation has not determined that information was viewed or copied from the system during the cyber incident, which occurred between November 24 and November 26, 2022, it has been unable to conclusively rule out such activity. Therefore, in an abundance of caution, QBH is taking steps to review the potentially affected data to determine the type of information present and to whom it relates. While this process was ongoing and prior to determining precisely what information was on the relevant systems, QBH provided notice of this incident on its website beginning on December 26, 2022 and issued notice to statewide media in Washington on the same date. Through its ongoing review, to date, QBH has identified certain individuals whose information was present in the environment at the time of the incident. On January 20, 2023, QBH confirmed that these individuals include two thousand seven hundred and fifty-two (2,752) Washington residents.

The information present on the system at the time of the incident may include name; contact information; demographic information; Social Security number; driver's license number or state identification card number; financial account information; date of birth; student, military, or passport identification number; health insurance policy number or health insurance identification number; health insurance information; medical history; mental or physical condition; medical diagnosis; treatment information.

Notice to Washington Residents

On or about January 25, 2023, QBH provided written notice of this incident to two thousand seven hundred and fifty-two (2,752) 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 learning that it was experiencing a cyber incident, QBH promptly took steps to secure its systems and investigate the full scope of the incident. While the response to the incident is ongoing, QBH has taken additional steps to further enhance the security of its systems. In an abundance of caution, it will be notifying individuals and providing information on steps individuals may take to protect information from misuse. Notification includes 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, one's state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Further, QBH notified federal law enforcement regarding the incident. QBH is providing access to credit monitoring services for twelve (12) months, through Experian, to individuals receiving notice at no cost to these individuals. QBH 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. QBH is also notifying the U.S. Department of Health and Human Services pursuant to the Health Insurance Portability and Accountability Act.

EXHIBIT A

quality behavioral health

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

January 25, 2023

i9248-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Re: Notice of [Extra1]

Dear Sample A. Sample:

Quality Behavioral Health ("QBH") is writing to make you aware of an incident that may affect your personal information. This letter provides you with information about the incident, what we are doing in response, and steps you may take to protect your personal information, should you feel it appropriate to do so.

What Happened? On November 26, 2022, QBH learned that it was experiencing a cyber incident. We promptly took steps to secure our systems and commenced an investigation into the nature and scope of the incident. We have been working diligently to investigate the incident and confirm any information that may be affected. While the investigation has not determined that information was viewed or copied from the system during the cyber incident, which occurred between November 24 and 26, 2022, we were unable to conclusively rule out such activity. Therefore, in an abundance of caution, we took steps to review the potentially affected data to determine the type of information present and to whom it relates. You are receiving this notice because we determined that your information was on the system at the time of the incident.

What Information Was Involved? The information present on the system at the time of the incident may include: name; contact information; demographic information; Social Security number; driver's license number or state identification card number; financial account information; date of birth; student, military, or passport identification number; health insurance policy number or health insurance identification number; health insurance information; medical history; mental or physical condition; medical diagnosis; treatment information. We note that the information varies by individual and not all of these data types were potentially affected for each person.

What We Are Doing. Upon learning of this incident, we promptly took steps to secure our systems and investigate the full scope of the issue. While our response to the event is ongoing, we have taken additional steps to further enhance the security of our systems. In an abundance of caution, we are also notifying you, and providing information on steps you may take to best protect your information, should you feel it is appropriate to do so. We are also offering you access to credit monitoring and identity theft protection at no cost to you as an added precaution. Information on how to enroll in these services may be found in the attached "Steps You Can Take to Help Protect Personal Information."

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefit forms and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the information contained in the attached "Steps You Can Take to Help Protect Personal Information" and to enroll in the credit monitoring and identity theft protection services we are making available to you.

For More Information. If you have additional questions, please call our assistance line at 1-833-769-0662, from 8:00 a.m. - 5:00 p.m. PST, Monday through Friday (excluding major U.S. holidays). You may also write to us at Quality Behavioral Health, 900 7th Street, Clarkston, WA 99403.

Sincerely,

Quality Behavioral Health
Compliance Officer
www.qbhs.org

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for 12 months.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 12-month membership. This product provides you with identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by April 30, 2023** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**: **ABCDEFGHI**

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 **(888) 397-0061** by April 30, 2023. Be prepared to provide engagement number **B084399** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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.[1]
- **Credit Monitoring:** Actively monitors Experian file 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[TM]:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] 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.

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.

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	833-395-6938
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 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.