





PO Box 480149
Niles, IL 60714

<<First Name>> <<MI>> <<Last Name>> <<Suffix>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:

Or Visit:
<https://response.idx.us/CHS>

February 8, 2024

<<VARIABLE HEADER FIELD>>

Dear <<First Name>> <<MI>> <<Last Name>> <<Suffix>>:

Perry Johnson & Associates, Inc. (“PJ&A”) is writing to inform you of an event that may impact the security of certain information it maintains on behalf of its business partners, including Concentra Health Services, Inc. (“Concentra”). This event had no impact on Concentra’s systems and was not the result of any activities or inactions on Concentra’s part. Rather, you are receiving this letter because PJ&A experienced an event that impacted certain information it maintains related to Concentra’s patients, including you. This notice provides information about the event, our response, and resources available to you to help protect your information from possible misuse, should you feel it is necessary to do so.

What Happened? PJ&A is a vendor that provides medical transcription services to healthcare organizations across the country, including Concentra. On May 2, 2023, PJ&A became aware of suspicious activity in its systems. PJ&A launched an investigation, with the assistance of third-party cybersecurity specialists, to determine the nature and scope of the event. The investigation determined that between March 27, 2023 and May 2, 2023, an unauthorized actor gained access to certain PJ&A systems and that information contained within those systems was accessible to the unauthorized actor. The investigation also determined that on or about April 7, 2023, and April 19, 2023, the unauthorized actor gained access to a system containing information related to Concentra patients.

PJ&A reviewed the potentially impacted data to identify the specific individuals with information that was potentially accessible during the event. Once complete, PJ&A notified Concentra of the event, as required, and provided Concentra with a list of its potentially impacted patients. Concentra promptly launched its own investigation and worked as quickly as possible to validate the results of PJ&A’s review and locate missing address information. Concentra completed this process recently, and then we moved as quickly as possible to notify you of same.

What Information Was Involved? The types of information related to you that were potentially accessible during the event include your name, address, <<Variable Text 1 (data elements)>>.

What We Are Doing. The confidentiality, privacy, and security of information in our care are among our highest priorities. Upon becoming aware of the event, we moved quickly to investigate and respond to the event, assess the security of our systems, and notify potentially affected individuals. We are notifying potentially affected individuals, including you, so that you may take further steps to best protect your information, should you feel it is necessary to do so. We regret any inconvenience or concern this event may cause. As an added precaution, we are offering credit monitoring services through IDX for <<Variable Text 2 (credit monitoring)>> months, at no cost to you.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, credits reports, and explanation of benefits forms for suspicious activity and to report any suspicious activity promptly to your bank, credit card company, healthcare provider, health insurance provider, or other applicable institution. Additional information and resources are included in the enclosed *Steps You Can Take To Protect Personal Information*. You may also enroll in the complimentary credit monitoring services available to you. Enrollment instructions are attached to this letter.

For More Information. We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call the dedicated assistance line at (888) 863-6260, Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time, excluding major U.S. holidays. Please have this letter ready if you call. Again, we take the privacy and security of information in our care very seriously and sincerely regret any inconvenience or concern this event may cause you.

Sincerely,
Perry Johnson & Associates, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring Services

We are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<Variable Text 2 (credit monitoring)>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling (888) 863-6260 or going to <https://response.idx.us/CHS> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8:00 a.m. to 8:00 p.m. Central Time. Please note the deadline to enroll is May 15, 2024.

- 1. Website and Enrollment.** Go to <https://response.idx.us/CHS> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.
- 3. Telephone.** Contact IDX at (888) 863-6260 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

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; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 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 <<#>> Rhode Island residents that may be impacted by this event.