

Appendix

Thrive Physical Therapy Partners (“Thrive”) recently completed its investigation into an email phishing incident that led to unauthorized access to two employee email accounts. Thrive first learned about the incident on June 26, 2025, after detecting unusual emails sent from one of the accounts. Upon confirming that the emails were sent without the employee’s knowledge, Thrive immediately secured the account and launched an investigation. Through the investigation, Thrive determined that two employees inadvertently disclosed their email account credentials in response to phishing emails they believed to be legitimate. As a result, an unauthorized party accessed the two email accounts between June 25, 2025 and June 26, 2025. While the likely purpose of the unauthorized access was to fraudulently obtain funds from Thrive rather than to access personal information, the unauthorized party did view certain emails, attachments, and SharePoint files. Thrive reviewed the emails, attachments, and SharePoint files that were accessed and determined that some contained names and Social Security numbers. On September 22, 2025, Thrive determined that some of this information pertained to 5 Nebraska residents.

On October 3, 2025, Thrive mailed notification letters via United States Postal Service First-Class mail to individuals whose information was involved, including to 5 Nebraska residents, in accordance with Neb. Rev. Stat. § 87-803. A copy of the notification letter is enclosed. Thrive offered individuals whose Social Security numbers may have been involved complimentary credit monitoring and identity protection services. Thrive also established a dedicated, toll-free incident response line to answer questions that individuals may have about the incident.

To help prevent something like this from happening again, Thrive is providing additional cybersecurity training to its staff.



Secure Processing Center
P.O. Box 680
Central Islip, NY 11722-0680

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

Thrive Physical Therapy Partners (“Thrive”) provides practice management services to physical therapy clinics and is committed to protecting the confidentiality and security of the information we maintain. We are writing to let you know about an email phishing incident that involved some of your information. This letter explains the incident, measures that have been taken, and some steps you can take in response.

Thrive recently completed its investigation into an email phishing incident that led to unauthorized access to two employee email accounts. We first learned about the incident on June 26, 2025, after detecting unusual emails sent from one of the accounts. Upon confirming that the emails were sent without the employee’s knowledge, we immediately secured the accounts and launched an investigation.

Through our investigation, we determined that two employees inadvertently disclosed their email account credentials in response to phishing emails they believed to be legitimate. As a result, an unauthorized party accessed two email and SharePoint accounts between June 25, 2025 and June 26, 2025. Although the likely purpose of the unauthorized access was to fraudulently obtain funds from Thrive, not to access personal information, the unauthorized party did view certain emails, attachments, and SharePoint files. Thrive conducted a thorough review of the accessed content and determined that one or more items contained your information, which may have included your name and Social Security number.

As a precaution, we are offering you complimentary membership to <<CM Duration>>-year of Epiq Privacy Solutions ID credit monitoring. This product is designed to detect potential misuse of your information and offers identity protection solutions aimed at promptly identifying and resolving any instances of identity theft. Activating this product will not impact your credit score. For more information on identity theft prevention and Epiq Privacy Solutions ID, including instructions on how to activate your services, as well as some additional steps you can take in response, please review the pages that follow this letter.

We deeply regret any inconvenience or concern this incident may cause and take this matter seriously. To help prevent something like this from happening again, we are providing additional cybersecurity training for our staff. If you have any questions about this incident, please call 855-291-2518, Monday through Friday, between 8:00 a.m. – 8:00 p.m., Central Time, excluding major U.S. holidays.

Sincerely,

Brad Ulrich

Brad Ulrich
Chief Executive Officer



<<Full Name>>
Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>
Coverage Length: <<CM Duration>> Year

Epiq - Privacy Solutions ID 3B Credit Monitoring

How To Enroll:

- 1) Visit www.privacysolutionsid.com and click “Activate Account”
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form
- 3) Complete the identity verification process
- 4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
- 5) Enter your log-in credentials
- 6) You will be directed to your dashboard and activation is complete!

Privacy Solutions ID provides three bureau credit monitoring through Equifax, credit report and score access, \$1 million identity theft insurance with \$0 deductible, ID Restoration services, and dark web monitoring. See below for more details.

Credit Monitoring with Alerts

Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

3-Bureau Credit Score and Report¹

Annual 3-Bureau VantageScore and 3-Bureau Credit Report

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, and payment platform, with alerts.

Dark Web Monitoring

Searches for compromised information across the dark web, with alerts.

Credit Report Lock/Freeze

Assists with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Lost Wallet Assistance

Assistance with canceling and reissuing credit and ID cards.

Identity Restoration

Dedicated ID restoration specialists who assist with ID theft recovery.

Up to \$1MM Identity Theft Insurance²

Provides up to \$1,000,00 (\$0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT²

Provides up to \$1,000,000 (\$0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity--occurrence based.

Personal Info Protection

Helps users find their exposed personal information on the surface web—specifically on people search sites and data brokers – so that the user can opt out/remove it. Helps protect members from ID theft, robo calls, stalkers, and other privacy risks.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 3B Credit Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

¹ The credit scores provided are based on the VantageScore 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness. Credit monitoring from Experian and TransUnion will take several days to begin.

² Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions, and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant of incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com/get-credit-report, 1-833-799-5355

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit. *How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com
- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com/credit-freeze

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. *How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Thrive's mailing address is 111 E Wacker Dr #1230, Chicago, IL 60601 and its phone number is (312) 676-4916.

Additional information for residents of the following states:

New York Residents: You may contact and obtain information from these state agencies: New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

North Carolina Residents: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov