

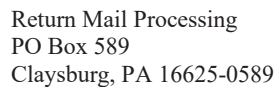
Appendix

On June 13, 2026, One Medical learned that an unauthorized person gained access to a third-party file-storage system used to retain archived information for One Medical Seniors, formerly known as Iora Health, which was acquired by One Medical in 2021. One Medical immediately took steps to secure the affected system and prevent further unauthorized access. These steps included revoking all user access and rotating credentials for all employees with access to the system. One Medical also launched an investigation and determined that, between June 8 and June 11, 2026, the unauthorized person was able to access patient files stored in this system.

This incident is limited to a file-storage platform used to store archived data from One Medical Seniors, formerly known as Iora Health. It does not impact other One Medical clinics or services, or the One Medical electronic medical record system.

One Medical's investigation identified a subset of impacted files related to certain legacy Iora Health and One Medical Seniors patients, and on June 17, identified the information of 16,884 Washington state residents within those files. The information involved varied by individual but may have included information commonly found in a clinical record, such as treatment plans, diagnostic information, imaging, and prescriptions, as well as demographic information, such as contact information, and information used for billing purposes, like a Medicare or Social Security Number.

On June 29, 2026, One Medical began mailing notification letters to the 16,884 Washington state residents via U.S First-Class mail. One Medical is offering two years of free credit monitoring services through Experian to all individuals involved. One Medical has also implemented additional safeguards to help prevent something like this from happening in the future.



 Q1065-L01-0000001 P001 T00001 *****SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01 OMS CUSTOMER
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

We take your trust seriously, and as part of our commitment to protecting patient information, we are sharing that we recently addressed a security event involving certain legacy Iora Health and One Medical Seniors information. This letter describes what happened, as well as the steps we have taken to protect the information in our care.

What information was involved: Our review has identified a subset of files from a certain number of legacy Iora Health and One Medical Seniors patients. We identified your information within those files. Given the personalized nature of our care, the information involved varied by individual, but may have included information commonly found in a clinical record, such as treatment plans, diagnostic information, imaging, and prescriptions, as well as demographic information, such as contact information, and information used for billing purposes, like a Medicare or Social Security Number.

What we are doing: We immediately took steps to secure the affected system and prevent further unauthorized access. This included revoking all user access and rotating credentials for all employees with access to the system. We have also implemented additional safeguards to help prevent something like this from happening in the future.

What you can do: We are here to support you. As a precaution and to encourage peace of mind, we are offering you a free two-year membership to Experian® IdentityWorksSM Credit 3B. Please refer to the enrollment information included with this letter. Enrolling in this service will not hurt your credit score.

If you need help activating your free credit monitoring membership or if you have questions about this incident, call **833-745-1398** from 7:00 a.m. – 7:00 p.m. in all continental U.S. time zones, except major holidays. You may also write to One Medical at privacy@onemedical.com.

Sincerely,
One Medical Seniors

0000001



To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

If you believe there was fraudulent use of your information as a result of this incident 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 24 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 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** September 30, 2026 by 11:59 pm UTC (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit3b>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team by September 30, 2026 at 833-745-1398 Monday – Friday, 7 am – 7 pm in all continental U.S. time zones (excluding major U.S. holidays). Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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.*
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files 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™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** 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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for 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 1000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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.identitytheft.gov

Information on Fraud Alerts and Credit or Security Freezes:

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 is because most creditors need to see your credit report before they approve a new account. If they cannot 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 160, Woodlyn, PA 19094, www.transunion.com

You will 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.