



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Allcare Medical Management Inc. contracts with healthcare organizations to provide medical practice management services. We place a high value on maintaining the privacy and security of the information we maintain for our customers. Regrettably, we are writing to let you know about a security incident that may involve some of your information, received in connection with the services Allcare provides for Family Planning Associates Medical Group, Inc. (“FPA”). This letter explains the incident, measures we have taken, and offers steps you can take in response.

What Happened? We recently detected suspicious activity relating to one of our employee’s email accounts. We immediately took steps to secure the account and a computer forensic firm was engaged to assist with our investigation. On May 23, 2024, the investigation determined that an unauthorized user accessed the email account for brief periods of time between March 4 and April 20, 2024. Based on the investigation, the likely purpose of the unauthorized access to the email account was to perpetuate an email phishing scheme, not to access personal information. However, we could not rule out the possibility that emails and attachments in the email account may have been viewed or acquired as a result of this incident. Therefore, we completed a detailed review of the email account’s contents, which was completed on June 12, 2024.

What Information Was Involved? Our review determined that some of your information was contained within the impacted email account and may have included one or more of the following: name, Social Security number, contact information, date of birth, medical record number, health insurance information, and/or information related to care you received at FPA.

Our electronic medical record systems are separate from our email accounts and were **not** affected by this event.

What We Are Doing. Please know that we take this matter very seriously. To help prevent something like this from happening in the future, we are making additional security enhancements to our email environment. We also continue to provide email security training and education to our employees.

What You Can Do. In an abundance of caution, we are offering you a complimentary membership in Experian® IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft. IdentityWorksSM is completely free to you, and enrolling in this program will not hurt your credit score. We also encourage you to remain vigilant by reviewing statements you receive from your health insurer and healthcare providers. If you see charges for services you did not receive, please contact the insurer or provider immediately. **For more information on identity theft prevention and IdentityWorksSM, including instructions on how to activate your complimentary membership, please review the pages that follow this letter.**

For More Information. Allcare considers the health, safety, and privacy of our patients a top priority. We deeply regret any concern this incident may cause you. If you have any questions, please contact our dedicated, toll-free call center at 1-???-???-????, Monday through Friday from 6:00 a.m. to 3:30 p.m. Pacific Time, excluding major U.S. holidays.

Sincerely,

Chad Tucker
Vice President

Activate IdentityWorks In Three Easy Steps

- **ENROLL** by <<b2b_text_6 (activation deadline)>> (Your code will not work after this date.)
- **VISIT** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bcredit>
- **PROVIDE** your **Activation Code**: <<activation code s_n>>

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 **TFN** by <<b2b_text_6 (activation deadline)>>. Be prepared to provide engagement number <<b2b_text_1 (engagement #)>> 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.*

- **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.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 at **TFN**. 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 (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).

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* 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

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'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:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

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.