



<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

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

<<b2b_text_1 (NOTICE OF SECURITY INCIDENT or DATA BREACH)>>

Dear <<First_name>> <<Last_name>>:

Doctor Alliance writes to inform you of a security event that may have impacted some of your personal information. Doctor Alliance hosts software that manages documents and performs certain billing functions for healthcare providers. One of our customers is AccentCare, which has provided services to you in the past. We received some of your personal information as part of the support we provide to AccentCare.

What Happened? On November 16, 2025, Doctor Alliance discovered an unauthorized third party had accessed our web application. Outside specialists were promptly engaged to help re-secure our systems and investigate the nature and scope of the intrusion. The investigation subsequently determined that an unauthorized third-party gained access to our web application from October 31, 2025, to November 16, 2025. The investigation did determine that certain files may have been accessed and/or exfiltrated by the unauthorized third party. We have since completed a comprehensive review of the files that may have been affected to determine what information was involved.

What Information Was Involved? The review determined that your name and the following information was contained within the potentially impacted files: Social Security number, Medical Record Number, Medicare Number, Diagnosis/Treatment Information, Provider Details, Medical Information, and Health Information.

What Are We Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. We moved quickly to respond and investigate the suspicious activity, assess and secure our network, and notify potentially impacted parties.

What You Can Do. While we have not been advised that any personal information has been used to commit identity theft or fraud, we recommend you take precautions, and *we are offering you <<ServiceTerminMonths>> months of free credit monitoring and \$1 million in identity theft insurance through Experian. You must activate the free product by the activation date in order for it to be effective. The activation instructions are included with this notification.*

We also recommend that you review the statements you receive from your healthcare providers and health insurer. If you were to see any charges for services you did not receive, please call your provider or insurer. We also have included some additional steps you may wish to take to protect yourself, as you deem appropriate.

For More Information. We understand you may have questions about this event not addressed in this letter. If you have any questions, you may contact our dedicated toll-free assistance line at (844) 443-1612, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding U.S. holidays

Sincerely,

Doctor Alliance

STEPS YOU CAN TAKE TO HELP PROTECT PERSON INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for <<ServiceTerminMonths>>-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 <<ServiceTerminMonths>>-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 <<ServiceTerminMonths>>-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** <<b2b_text_6 (activation deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: <<Activation Code s_n>>

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 at (877) 288-8057 by <<b2b_text_6 (activation deadline)>>. Be prepared to provide engagement number <<b2b_text_2 (engagement #)>> as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR <<ServiceTerminMonths>>-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 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™:** 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.

ADDITIONAL STEPS YOU MAY WISH TO TAKE

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD AND IDENTITY. CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your credit reports, debit/credit card, insurance policy, bank account and other account statements for unauthorized activity— especially over the next 24 months. Activate alerts on your bank accounts to notify you of suspicious activity and change passwords/security verifications as needed – particularly if same password is used over multiple online accounts. If your medical information was involved, it is also advisable to review the billing statements you receive from your healthcare providers. Immediately report suspicious activity, fraudulent charges, or suspected identity theft in your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider and law enforcement, including FTC and/or your State Attorney General.

➤ **FREEZE YOUR CREDIT FILE.** You have a right to place a ‘security freeze’ on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. Security freeze generally does not apply to existing account relationships and when a copy of your report is requested by existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. It is free to place, lift, or remove a security freeze. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze:

- *Equifax*, PO Box 105788, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver’s license or ID card, military ID, etc.); and if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

➤ **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

➤ **ORDER FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) copies of your credit report, free of charge. You must contact each of the 3 credit reporting agencies directly to obtain such additional reports.

- *Equifax*, PO Box 105281, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

➤ **SUMMARY OF YOUR RIGHTS UNDER FAIR CREDIT REPORTING ACT (FCRA):** FCRA promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. (1) You must be told if information in your file has been used against you. (2) You have the

right to know what is in your file. (3) You have the right to ask for a credit score. (4) You have the right to dispute incomplete or inaccurate information. (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. (6) Consumer reporting agencies may not report outdated negative information. (7) Access to your file is limited. (8) You must give your consent for reports to be provided to employers. (9) You may limit “prescreened” offers of credit and insurance you get based on information in your credit report. (10) You have a right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. (11) You may seek damages from violators. (12) Identity theft victims and active-duty military personnel have additional rights.

➤ **CONTACT LAW ENFORCEMENT, FEDERAL TRADE COMMISSION (FTC), AND STATE ATTORNEY GENERAL.** 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 law enforcement, the FTC and/or the Attorney General’s office in your home state. You may also contact these agencies for information on fraud alerts and security freezes and how to prevent or minimize the risks of identity theft. You may contact the FTC at www.ftc.gov/idtheft; FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.

➤ **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM YOUR STATE ATTORNEY GENERAL.**

- **Connecticut:** You may contact and obtain information from Connecticut Attorney General’s Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
- **District of Columbia:** You may contact and obtain information from Office of the Attorney General for the District of Columbia, 400 6th Street, NW, Washington, DC 20001, 1-202-727-3400, databreach@dc.gov, www.oag.dc.gov.
- **Iowa:** You are advised to report any suspected identity theft to law enforcement or Iowa Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, <https://www.iowaattorneygeneral.gov>, 515-281-5926 or 888-777-4590.
- **Maryland:** You may contact and obtain information from your state attorney general at Maryland Attorney General’s Office – Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-410-576-6300; <https://www.marylandattorneygeneral.gov/> Consumer Hotline 1-410-528-8662, or consumer@oag.state.md.us. Contact information for Doctor Alliance is as follows: Doctor Alliance, 750 North St. Paul Street Suite 250, Dallas, TX 75201, info@doctoralliance.com, (800)-608-5368.
- **Massachusetts:** You may contact and obtain information from Office of Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html. The mitigation services outlined above are offered pursuant to Mass. Gen. Laws Ann. Ch.93H, § 3(b). You also have the right to request a police report about this incident if one exists.
- **New York:** You may contact and obtain information from 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 Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.
- **North Carolina:** You may contact and obtain information from North Carolina Attorney General’s Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov.
- **Rhode Island:** You may contact and obtain information from Rhode Island Attorney General Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov. <<b2b_text_3 ([RI Resident Number] Rhode Island residents were impacted by this incident.)>>