

20458

Zocdoc

May 28, 2021

Dear Zocdoc User,

Notice of Data Breach

At Zocdoc, we understand how important your personal information is, and we work hard to protect it. Out of an abundance of caution and in compliance with regulatory requirements, we are writing to inform you that some past or current staff members at medical or dental practices where you previously booked an appointment may have had access to Zocdoc's system, which contains your personal information (as detailed in the "What Information Was Involved" section of this letter), after their authorization was changed or revoked. **Importantly, we have no reason to believe, at this time, that your personal information has been misused in any way.**

What Happened

As you know, Zocdoc allows you to book appointments with doctors who list available appointment times at their medical or dental practices on our platform. Each practice registered with Zocdoc receives usernames that allow staff members to access Zocdoc's system (the "Provider Portal"), and view appointments and other information you provide when booking an appointment. Beginning in August 2020, we learned of programming errors that allowed some past or current practice staff members to access the Provider Portal after their usernames and passwords were intended to be removed, deleted or otherwise limited. Notably, these practices and their current and former staff members have direct obligations to maintain the security and confidentiality of the personal information of their patients, and we have no reason at this time to believe that your information was disclosed outside of these practices and staff members.

We have notified each practice affected by these errors so that they may conduct an internal assessment as an additional precaution. It is possible that you may receive a separate notification from these practices (or the health system with whom they are affiliated).

What Information Was Involved

To the extent that any personal information was accessed, it would include your: name, email address, phone number, and appointment history (i.e. the times and dates of your past appointments) with that practice, and additional information such as insurance member ID, social security number, and any relevant medical history that you may have provided to the practice via Zocdoc in connection with an appointment booked through our service. If you used your Zocdoc account to book an appointment for another individual, or referenced a primary or secondary insurance holder other than yourself on your check-in forms, any personal information you provided about these individuals may also have been accessible.

Zocdoc

It is important to note that the following types of information could **not** have been accessed, because Zocdoc does not collect or store such information: credit card numbers, debit card or PIN numbers, bank account information, radiological or diagnostic reports, or any medical records from a healthcare provider regarding your treatment.

What We Are Doing

As soon as we learned of these programming errors, we launched a thorough investigation of our software and code. We repaired these errors, and the affected usernames can no longer access our system. We have also strengthened our security practices and are taking appropriate steps to prevent an incident like this from recurring. We will continue to regularly audit our system security and take action to enhance it.

As a precautionary measure to safeguard your information from potential misuse, we are partnering with Experian to provide its Experian IdentityWorks product to you for 24 months at no charge. A description of this product is provided in the attached material, which also contains instructions about how to enroll with your activation code (and if applicable, activation code(s) for other individual(s) whose personal information you provided through your Zocdoc account). If you choose to take advantage of the Experian IdentityWorks product, it will provide you with identity theft detection and resolution of identity theft services as described in the attached material. In order for us to activate this service, you must complete the enrollment process by September 30, 2021.

What You Can Do

As noted above, there is no indication that your personal information has been misused in any way. However, out of an abundance of caution, we do advise that you remain vigilant for the next 12 to 24 months by regularly reviewing your financial and healthcare related accounts, monitoring free credit reports, and reporting any suspicious or unrecognized activity to the relevant financial or healthcare institution immediately.

You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free (877) 322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. We also encourage you to review the "General Information About Identity Theft Protection" sheet attached to this message.

For More Information

Zocdoc has made available a toll-free number for consumers to call if they have any questions or wish to obtain additional information. You can contact us at (844) 310-0643 from 8:00am - 8:00pm EST, Monday through Friday, and 9:00am - 6:00pm EST on Saturday and Sunday. For

Zocdoc

more information on Zocdoc's information security practices, please visit:
<https://www.zocdoc.com/about/topic/data-privacy/>.

Zocdoc takes the protection of your information seriously, and we deeply regret any inconvenience that this may cause you. Please contact us at (844) 310-0643 or email us at service@zocdoc.com if you have any questions or concerns regarding this matter.

Sincerely,



Simon Mosk-Aoyama
Chief Technology Officer

Enclosures

Zocdoc

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

You should remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

Credit Reports. Under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf, and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
P.O. Box 105788 Atlanta, GA 30348 www.equifax.com (800) 525-6285	P.O. Box 9554 Allen, TX 75013 www.experian.com (888) 397-3742	P.O. Box 2000 Chester, PA 19016 www.transunion.com (800) 680-7289

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Place a Security Freeze on your Credit Report. You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line or a written request. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. You can place a freeze and lift a security freeze on your credit report free of charge.

Zocdoc

You may contact the Federal Trade Commission (FTC) and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the FTC and/or your state's attorney general office for information on how to prevent or avoid identity theft. You can contact the FTC at: **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20508, www.ftc.gov, 1-877-IDTHEFT (438-4338).

If you are a California resident, you may also wish to review the information provided by the California Attorney General at <https://oag.ca.gov/idtheft>.

If you are a District of Columbia resident, you may obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia by visiting <https://oag.dc.gov/consumer-protection>, emailing consumer.protection@dc.gov, calling (202) 442-9828, or mailing Office of the Attorney General, Office of Consumer Protection, 400 6th Street, NW Washington, DC 20001.

If you are an Iowa resident, state law advises you to report any suspected identity theft to law enforcement or to the Iowa Attorney General, Consumer Protection Division, 1305 E. Walnut St., Des Moines, IA 50319, 1-888-777-4590.

If you are a Maryland resident, you can contact the Maryland Office of the Attorney General, Consumer Protection Division at: 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

If you are a New Mexico resident, you have certain rights pursuant to the federal Fair Credit Reporting Act (FCRA). For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

If you are a New York resident, you can contact the New York Office of the Attorney General at www.ag.ny.gov, 1-800-771-7755; the New York Department of State, www.dos.ny.gov, 1-800-697-1220; and the New York Division of State Police, www.ny.gov/agencies/division-state-police, (914) 834-9111.

If you are a North Carolina resident, you can contact the North Carolina Office of the Attorney General, Consumer Protection Division at: 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226.

Zocdoc

If you are an Oregon resident, state law advises you to report any suspected identity theft to law enforcement or to the FTC.

If you are a Rhode Island resident, you can contact the Office of the Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov/>, (401) 274-4400 or file a police report by contacting (401) 444-1000.



**ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN
IDENTITYWORKS MEMBERSHIP:**

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: September 30, 2021 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your activation code: [REDACTED]

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 (877) 890-9332 by September 30, 2021. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the identity restoration services by Experian.

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 agents 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 (877) 890-9332. 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).

Zocdoc

Please note that this Identity Restoration support 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. 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.