May 16, 2016

Dear [Insert Name],

Notice of Data Breach

At Zocdoc, we understand how important your personal information is, and we work hard to protect it. For that reason, 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 - after their authorization changed. We are notifying you of this out of an abundance of caution, and to comply with regulatory requirements. **We have no indication, 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 their medical or dental practices on our service. Each practice registered with Zocdoc receives usernames which allow staff members to access Zocdoc's system (the "Provider Dashboard") to view appointments and other information you provide when you book an appointment. In June 2015, we learned of programming errors in the processes responsible for managing username access to the Provider Dashboard. This allowed some past or current practice staff members to access the Provider Dashboard, and therefore potentially view your personal information, after their usernames were removed, deleted or otherwise limited. Access may have occurred between [first access date] to [last access date]. These practices and their staff members had obligations regarding the secure and confidential handling of personal information.

What Information Was Involved

It is important to note that the following types of information could not have been accessed, as Zocdoc does *not* collect or store: credit card numbers, debit card or PIN numbers, bank account information, driver's license or state identification cards, radiological or diagnostic reports. Personal information that may have been accessed includes: name, email address, phone number, ["social security number, "]appointment history (times and dates of your appointments) with that practice, and if previously provided to that practice by you via Zocdoc, additional information such as insurance member ID and other medical history.

What We Are Doing

As soon as we learned of these programming errors, we launched a thorough investigation of our software and website. We quickly 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.

What You Can Do

As noted above, there is no indication that your personal information has been misused in any way. Out of an abundance of caution, and to help proactively protect against any potential misuse of your personal information, we have arranged a complimentary one-year membership of Experian's® ProtectMyID® Elite service. This helps detect possible misuse of your information and provides you with identity protection support. To enroll:

1. VISIT www.protectmyid.com/enroll
2. PROVIDE your activation code: [code]
3. ENSURE that you enroll by September 30, 2016 (Your code will not work after this date.)

We have provided additional details on this service below. If you have questions or need an alternative to enrolling online, please call Experian at 877-441-6943 and provide engagement #PC101240.

For More Information

Additionally, we encourage you to review the enclosed information about steps you can take to protect yourself. While no financial information was compromised, we encourage you to review your financial and healthcare related accounts, and report any suspicious or unrecognized activity immediately. As recommended by federal and state agencies, you should be vigilant for the next 12 to 24 months, and report any suspected incidents of fraud to the relevant financial or healthcare institutions.

We deeply regret any inconvenience that this may have caused you. We take the protection of your information seriously, and you can learn more about how we protect your privacy and keep your data safe at www.zocdoc.com/trust. Please contact us at 844-310-0643 if you have any questions or concerns regarding this matter.

Sincerely,

Anna Elwood, VP of Operations

Zocdoc, Inc.
568 Broadway, FL 9
New York, NY 10012

MORE INFORMATION ABOUT IDENTITY PROTECTION

We encourage you to consider the following proactive steps designed to detect and prevent financial fraud, identity theft or other misuse of your personal information:

Review your Credit Reports and Account Statements

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report once every 12 months by:

- Visiting http://www.annualcreditreport.com
- Calling toll-free at 877-322-8228, or
- Completing an Annual Credit Report Request Form (found at http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm) and mailing it to:

  Annual Credit Report Request Service
  P.O. Box 105281
  Atlanta, GA 30348-5281

You can also purchase a copy of your credit report by contacting one of the three national credit reporting companies:

Equifax (800) 685-1111 www.equifax.com P.O. Box 740241 Atlanta, GA 30374-0241	Experian (888) 397-3742 www.experian.com P.O. Box 9532 Allen, TX 75013	TransUnion (800) 916-8800 www.transunion.com P.O. Box 6790 Fullerton, CA 92834-6790

When you receive your credit reports, it is advised that you:

- Review them carefully.
- Look for accounts you did not open.
- Look for inquiries from creditors that you did not initiate.
- Look for personal information, such as home address and Social Security Number, that is inaccurate.

If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports. Promptly report any suspicious activity to us, and if you suspect any identity theft, report it to proper law enforcement authorities, including local law enforcement.

You may contact the national credit reporting agencies listed above to learn about preventing identity theft and to obtain additional information about avoiding identity theft. All U.S. residents may also contact the Federal Trade Commission ("FTC") for additional information at the following address:

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

Fraud Alerts

You may wish to consider placing a fraud alert to put your creditors and potential creditors on notice that you may be a victim of fraud. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-800-525-6285, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, www.transunion.com

Credit or "Security" Freezes

You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you put on a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift, and/or remove a credit freeze. The cost of placing, temporarily lifting, and removing a credit freeze also varies, generally $5 to $20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.*

The instructions for how to establish a credit freeze differ from state to state. Contact the three major credit reporting companies listed above (TransUnion, Experian, and Equifax) to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Consider Applying for an Identity Protection PIN with the IRS

An IP PIN is a six-digit number assigned to eligible taxpayers that helps prevent the misuse of your SSN on fraudulent federal income tax returns. If you know your SSN has been compromised, or are concerned that it may have been, obtaining an IP PIN from the IRS can help prevent someone from using your SSN to submit a fraudulent tax return without you knowing in order to steal a refund check.

Important: You are currently unable to opt out once you get an IP PIN. You must use an IP PIN to confirm your identity on all federal tax returns you file this year and in subsequent tax years. If you e-file your return and your IP PIN is missing or incorrect, the IRS will reject your return. Filing a paper return with a missing or incorrect IP PIN delays its processing. This is for your protection so the IRS can determine it's your return.

To get your IP PIN, you must verify your identity online at http://www.irs.gov/Individuals/Get-An-Identity-Protection-PIN. You will need to have immediate access to your email account to receive a confirmation code. You will receive your IP PIN online once the IRS verifies your identity. The IRS will then send you a new IP PIN each December by postal mail. If you move, you must submit a change of address form to the IRS.

Visit the IRS's online page of FAQs for more information and to determine whether the IP PIN might be right for you at: http://www.irs.gov/Individuals/Frequently-Asked-Questions-about-the-Identity-Protection-Personal-Identification-Number-(IP-PIN)

Warnings about Email and Phone Scams

Please be aware of scams involving emails, attachments, web links (phishing), and fake telephone calls. You should be on high alert. The following tips, although written with this particular incident in mind, reflect critical *do's and don'ts* when it comes to scams and hoaxes. It is good practice to follow these tips to avoid being victimized by online and telephone scams.

- DO NOT open any attachments that arrive with Zocdoc email.
- DO NOT provide any personal information over the phone if you receive a call from someone at Zocdoc.
- REPORT to Zocdoc if you have received any of these emails or phone calls.
- DO check your credit card and bank statements for any suspicious charges or entries.
- DO check your credit reports periodically.

What If You Find Evidence of Identity Theft or Other Suspicious Activity?

We recommend that you promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. The FTC provides useful information regarding identity theft and maintains a database of identity theft cases for use by law enforcement agencies. You may file a report with the FTC in the following ways:

- Calling the FTC's Identity Theft Hotline: 1-877-IDTHEFT (438-4338)
- Online at http://ftc.gov/idtheft, or
- By mail at:

  Identity Theft Clearinghouse
  Federal Trade Commission
  600 Pennsylvania Avenue, NW
  Washington, DC 20580

Additional useful information may be found at http://ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN® PROTECTMYID® ELITE MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- Free copy of your Experian credit report
- Surveillance Alerts for:
  - Daily 3 Bureau Credit Monitoring: Alerts of key changes & suspicious activity found on your Experian®, Equifax®, and TransUnion® credit reports.
  - Internet Scan: Alerts if your personal information is located on sites where compromised data is found, traded or sold.
  - Change of Address: Alerts of any changes in your mailing address.
- Identity Theft Resolution & ProtectMyID ExtendCARE: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- $1 Million Identity Theft Insurance*: Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.
- Lost Wallet Protection: If you misplace or have your wallet stolen, an agent will help you cancel your credit, debit, and medical insurance cards.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-441-6943.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). 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.*