

December 4, 2023

SID BOSE
DIRECT NUMBER: 317-236-2243
SID.BOSE@icemiller.com**CONFIDENTIAL****VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)**

Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Written Notification of a Data Breach

To Whom It May Concern:

On behalf of my client, Washington National Insurance Company, I am hereby submitting a written notification of a data breach, in compliance with Md. Code Ann. Comm. Law § 14-3504(h), that may have impacted **two (2)** Maryland residents.

Washington National uses a third-party vendor's software to operate one its websites, *My.WashingtonNational.com* (sometimes referred to herein as, the "Website"). On or around October 6, 2023, Washington National discovered a software issue involving the Website which may have exposed a limited amount of personal information to other registered users on *My.WashingtonNational.com*.

When Washington National first discovered the issue, it immediately engaged the vendor to identify the root cause and mitigate the issue, disabled certain website functions, and launched an investigation. As part of the investigation, Washington National, in coordination with the vendor, conducted analysis of all activity that occurred on the Website. In addition, Washington National directed the vendor to provide all information related to the software defect and any other information to assess whether any information may have been exposed.

After an expansive investigation with the vendor, the vendor informed Washington National that its software had a defect that could have caused, in very limited circumstances, a *My.WashingtonNational.com* user's information to be exposed to other registered *My.WashingtonNational.com* users. This defect would have impacted only a limited number of users, using certain types of devices to access the Website. The vendor also informed us that the software defect arose from an upgrade in the vendor's software, and may have existed since October 22, 2022. Washington National disabled the defective portion of the Website on October 6, 2023. After the vendor identified the defect in their software, the vendor promptly provided a fix to remedy the software defect. Additionally, the vendor has informed Washington National that it will conduct additional testing and validations prior to deploying any future upgrades. The

vendor will also test its upgrades to identify any possible defects that could give rise to similar issues and will mitigate such defects before the upgrade is released.

Through its investigation, Washington National determined that the potential exposure of personal information was related to past or pending claims for accident benefits including name, social security number, information about medical care and health plan, and documents to support accident claim details. At this time Washington National has no evidence that any of the potentially impacted personal information of the Maryland residents was actually improperly acquired, accessed, or viewed by another *My.WashingtonNational.com* user, nor does it believe that the Maryland residents are at any risk of fraud or identity theft.

Nonetheless, out of an abundance of caution, 2 Maryland residents are being notified of the breach. A copy of the notice that was sent to the affected Maryland residents on or around December 5, 2023, is attached herewith. Credit monitoring and identity theft protection services will be offered to the affected Maryland residents for a period of twelve (12) months.

If you require further information about this matter, please contact me by telephone at (317) 236-2243 or via email at Sid.Bose@icemiller.com.

Sincerely,

ICE MILLER, LLP



Sid Bose

Attachment: Individual Notification Letter Template

Washington National Insurance Company
Return to IDX:
4145 SW Watson Ave Suite 400
Beaverton, OR 97005

(Minor: <<To the Parent or Guardian or:>>)
<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

December 5, 2023

<<Variable Data 4>>

Dear (Minor: <<Parent or Guardian of>>) <<First Name>> <<Last Name>>,

At Washington National Insurance Company ("Washington National"), we take your privacy and security very seriously. We are writing to let you know about an incident which may have involved your personal information.

What Happened

On October 6, 2023, we discovered a software issue involving My.WashingtonNational.com which may have exposed a limited amount of your information to other registered users.

Washington National uses a third-party vendor's software to operate the My.WashingtonNational.com website. When we first discovered the issue, we immediately engaged the vendor to identify the root cause and mitigate the issue. After an expansive investigation with the vendor, the vendor informed us that its software had a defect that could have caused, in very limited circumstances, a My.WashingtonNational.com user's information to be exposed to other registered My.WashingtonNational.com users. This defect would have impacted only a limited number of users who used certain types of devices to access the My.WashingtonNational.com website. The vendor also informed us that the software defect arose from an upgrade in the vendor's software, and may have existed since October 22, 2022. After the vendor identified the defect in their software, the vendor promptly provided a fix to remedy the software defect.

What Information Was Involved

Through the investigation, we determined that the potential exposure of your information was related to <<Variable Data 5>> including <<Variable Data 6>>. While we have no evidence that your personal information was improperly acquired or accessed by another My.WashingtonNational.com registered user, or that you are at any risk of fraud or identity theft, we are notifying you out of an abundance of caution. <<Variable Data 7>>

What We Are Doing

When we discovered this issue on October 6, we immediately disabled certain website functions and launched an investigation. As part of our investigation, we engaged the vendor and conducted analysis of all activity that occurred on My.WashingtonNational.com. In addition, we directed the vendor to provide all information related to the software defect and any other information to assess whether your information may have been exposed. As noted above, we have no evidence that your personal information was improperly acquired or accessed by another My.WashingtonNational.com registered user, or that you are at any risk of fraud or identity theft.

In any case, we are notifying you out of an abundance of caution, and are offering identity theft protection services through IDX, a ZeroFox Company, a leader in data breach and recovery services. IDX identity protection services include:

<<12/24>> months of <<Variable Data 8>> CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time.

Please note the deadline to enroll is March 5, 2024. Please do not discard this letter as you will need to reference the Enrollment Code above to enroll in the services.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

You will find detailed instructions for enrollment on the enclosed Recommended Steps document.

Please call 1-800-939-4170 or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

Sincerely,

Washington National

(Enclosure)



Recommended Steps to help Protect your Information

1. Website and Enrollment. Scan the QR image or go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX identity protection, notify them immediately by calling or by logging into the IDX website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of the IDX ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. Office of the Attorney General of California, 1300 I Street, Sacramento, CA 95814, Telephone: 1-800-952-5225.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, <https://consumer.ftc.gov>, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.