



April 13, 2023

VIA EMAIL AND USPS CERTIFIED MAIL

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Data Security Incident

Dear Attorney General Formella:

We write on behalf of NationsBenefits Holdings, LLC, a leading provider of supplemental benefits, flex cards, and member engagement solutions to healthcare plans and managed care organizations. NationsBenefits, along with more than 100 other organizations, was recently the victim of a security incident resulting from a zero-day remote code execution vulnerability in Fortra, LLC's ("Fortra") GoAnywhere managed file transfer ("MFT") software. On behalf of NationsBenefits and the NationsBenefits customers listed below, we write to provide you notice of the incident and inform you that New Hampshire residents were impacted. This letter also explains the steps that have been taken to address the incident.

What Happened? On or around January 30, 2023, at 12:35:30 UTC, a cyber threat actor(s) exploited the zero-day vulnerability—now known as CVE-2023-0669—to access a NationsBenefits GoAnywhere server. This incident was first discovered by NationsBenefits on February 7, 2023, at approximately 16:02 UTC, when NationsBenefits' security monitoring team received an alert regarding a potential security event on the impacted MFT server. NationsBenefits promptly contacted Fortra to assist in the investigation of the event. Upon initial review, Fortra advised NationsBenefits that it appeared that NationsBenefits' instance of GoAnywhere had been subject to unauthorized access as a result of the zero-day vulnerability targeting Fortra's MFT software. The incident at NationsBenefits was limited to two MFT servers; there is no evidence that the threat actors moved laterally to other applications or systems within the NationsBenefits environment.

What Information was Impacted? The information involved in the incident included the following data elements of some health plan members:

Not every individual affected had all of these data elements impacted, or the same combination of data elements impacted.

The NationsBenefits customers whose impacted plan members include New Hampshire residents include:

<u>Plan</u>	<u>Impacted Residents</u>
Aetna ACE	appx. 7,001 residents
Elevance Health Flexible Benefit Plan	appx. 6 residents
UAW Retiree Medical Benefits Trust	appx. 123 residents

Steps NationsBenefits has taken. Upon discovering that Fortra was experiencing a security incident, NationsBenefits took steps to secure its GoAnywhere server by immediately taking it offline and launching an investigation, which is being conducted by McDermott Will & Emery LLP and a leading cybersecurity firm. NationsBenefits also promptly notified the Federal Bureau of Investigation (“FBI”) and has worked cooperatively with the FBI’s investigation into this cyberattack on Fortra and many of its GoAnywhere customers.

The NationsBenefits environment was scanned with multiple security tools and confirmed that the threat actor(s) did not access any applications or systems beyond the Fortra GoAnywhere MFT environment. NationsBenefits has taken its GoAnywhere server permanently offline and implemented a new file transfer solution that does not rely on Fortra software. NationsBenefits implements a comprehensive, written security and privacy program that includes technical, physical, and administrative safeguards. Even prior to the zero-day vulnerability becoming known, NationsBenefits’ layered security controls blocked certain malicious activity, limiting the impact of this incident.

NationsBenefits has been in frequent communications with its impacted clients to support all impacted covered entities’ response efforts. NationsBenefits immediately began its investigation and notified potentially impacted clients on a rolling basis beginning on February 9, 2023. NationsBenefits first confirmed that personal information was impacted beginning on or around February 13, 2023, and on an ongoing basis thereafter as its investigation progressed.

At the request and under the authorization of its impacted clients, NationsBenefits began notifying impacted plan members on April 13, 2023. Impacted members will receive written notice, which for most members will be substantially similar to the enclosed notification letter template. Members of

Attorney General John Formella
April 13, 2023
Page 3

certain impacted plans will also receive substitute notice through the NationsBenefits website at <https://nationsbenefits.com/incidentsupport>. NationsBenefits is providing complimentary 24-month membership to Experian's® IdentityWorksSM for members with sensitive data impacted or where otherwise deemed reasonable and appropriate by NationsBenefits' clients. NationsBenefits is also providing required notices to the H.H.S. Office for Civil Rights, prominent media outlets, consumer reporting agencies, and certain state agencies.

For more information: Please do not hesitate to contact us if you have any questions regarding this letter. You may also contact our impacted customers directly at:

Sincerely,

Robert Duffy
Enclosures

**McDermott
Will & Emery**



[Experian Return Address Line 1]

[Experian Return Address Line 2]

[first_name] [last_name]

[address_1]

[address_2]

[city], [state_province] [postal_code]

[Letter_Date]

Dear [Full_Name]:

NationsBenefits Holding, LLC, and its affiliates and subsidiaries (collectively, “NationsBenefits” or “we”), provides benefits administration services to your health insurer, [client_name]. We place a high value on maintaining the privacy and security of the information we maintain for our health plan customers. Regrettably, this letter is to inform you that a vendor we used to exchange files with [client_name] was recently the victim of a cybersecurity attack, which impacted some of your personal information. We notified [client_name] of this incident on [customer_notice_date]. This letter explains the incident, the measures we have taken in response and the steps you can take.

What Happened? NationsBenefits used software provided by a third-party vendor, Fortra, LLC (“Fortra”), to securely exchange files with your health plan. On or around January 30, 2023, Fortra experienced a data security incident in which a malicious actor(s) accessed or acquired the data of multiple organizations, including NationsBenefits. When we learned of this incident on February 7, 2023, we immediately took steps to secure our systems and launched an investigation, which was conducted by an experienced outside law firm and a leading cybersecurity firm. As part of our investigation, NationsBenefits analyzed the impacted data to determine whether any individual’s personal information was subject to unauthorized access or acquisition. On [Discovery_Date], NationsBenefits confirmed that, unfortunately, some of your personal information was affected by the incident.

What Information Was Involved? The personal information involved included your [data_elements].

What Are We Doing? Data privacy and security are among our highest priorities, and we have extensive measures in place to protect information entrusted to us. Upon discovering the incident, we immediately took steps to mitigate the risk to our clients and personal information. We immediately stopped using Fortra’s software and worked with experienced legal counsel and a leading cybersecurity firm to conduct a comprehensive investigation of the incident. We also notified law enforcement authorities. To help prevent similar incidents from happening in the future, we have implemented and are continuing to implement additional procedures to further strengthen the security of our IT system environments.

What Can You Do? We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your free credit reports for suspicious activity and to detect errors. Enclosed with this letter are some steps you can take to protect your information.

As a measure of added security and to help protect your identity, we are offering a complimentary 24-month membership to Experian’s® IdentityWorksSM. This product provides you with credit monitoring, identity theft resolution services, and \$1,000,000 of identity theft insurance. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by:** July 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>

- Provide your **activation code**: [code]

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 833-420-2834 by July 31, 2023. Be prepared to provide engagement number [engagement #] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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 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 personal information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-420-2834. 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).

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.

For More Information. We regret that this incident occurred and any concern it may cause you. If you have additional questions, please call our dedicated, toll-free call center at 833-420-2834, Monday through Friday between 9:00 a.m. and 11:00 p.m. and Saturday and Sunday between 11:00 am and 8:00 pm Eastern Time, excluding major U.S. holidays.

Sincerely,

Glenn M. Parker MD
CEO & Founder

* 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.

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.

Credit Freezes (for Non-Massachusetts Residents): 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 place 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. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, 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.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as indicated above.

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.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the respective address indicated above.

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse’s credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver’s license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). If you have been a victim of identity theft, and you provide

the credit reporting agency with a valid police report, the agency cannot charge you to place, lift or remove a security freeze. In all other cases, the credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze.

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 about 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 Connecticut resident, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

If you are a District of Columbia resident, you may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

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 Massachusetts resident, under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

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.

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 have the right to obtain a police report. You also have the right to request a security freeze, as described above. You can also 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.

If you are a West Virginia resident, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.