CONDUENT

100 Campus Drive, Suite 200
Florham Park, NJ 07932

January 19, 2021

Office of the New Hampshire Attorney General
Consumer Protection Bureau
33 Capital Street
Concord, NH 03301

To Office of the New Hampshire Attorney General:

On behalf of Conduent, Inc, I am writing to inform you of recent security breach in accordance with N.H. Rev. Stat. § 358-A which involved one (1) resident from New Hampshire.

On October 6, 2020, Conduent began an investigation after receiving reports of unauthorized account withdrawals. We identified questionable system activity that included change of email address and bank account details, leading to unauthorized transactions. One (1) New Hampshire resident was affected by this fraudulent activity.

The unauthorized account changes and withdrawals are believed to have occurred between May 7, 2019 through October 28, 2020. We identified the individual responsible for making these unauthorized account activities as an internal employee. This individual is no longer employed, and access has been removed from all applications, systems, and premises.

The data elements exposed include the member's name, email address, payee names and addresses, personal banking information, HSA account number, last 4 digits of HSA debit card, tax forms (1099SA and 5498SA) which included the last 4 digits of social security number, investment information, and security questions.

Affected individuals were notified on November 25, 2020 and attached is a sample letter. In addition, Conduent offered to provide one year of free credit monitoring for impacted customers.

Conduent takes the responsibility to protect its customers' privacy very seriously and has taken steps to increase quality assurance and monitoring of employee activities to prevent this from happening again.

Please contact us with any questions or concerns.

Sincerely,

Brian Clayton
Brian Clayton
Associate General Counsel
Conduent. Inc.

BenefitWallet®

11/25/2020

Re: Information regarding your account ending in XXXX

Notice of Data Breach

Our records indicate that we administer one or more of your Health Savings Accounts (HSA) and are writing to inform you of a security breach that involved an unauthorized use and disclosure of your personal information.

WHAT HAPPENED:

On October 6, 2020, we began an investigation after receiving reports of some unauthorized account withdrawals. We identified some questionable system activity such as change of email address and bank account details, leading to unauthorized transactions. Your account was identified as one of the accounts affected by this unauthorized and fraudulent activity.

We identified patterns and closed some accounts to prevent further fraud. In other cases, we were able to stop some of the unauthorized transactions.

The unauthorized account changes and withdrawals are believed to have occurred between May 7, 2019 through October 28, 2020. We also identified the individual responsible for making these unauthorized account activities as an internal employee. This individual is no longer employed, and access has been removed from all applications, systems, and premises.

WHAT INFORMATION WAS INVOLVED:

This individual had access and used or attempted to use your personal information to make unauthorized changes and fraudulent withdrawals from your account. The personal information included your name, email address, payee names and addresses, personal banking information, HSA account number, last 4 digits of HSA debit card, tax forms (1099SA and 5498SA) which included the last 4 digits of social security number, investment information, and security questions.

WHAT ARE WE DOING:

We activated our corporate security investigations team, involved legal, business operations, human resources, privacy, and computer security investigation response groups. This individual is no longer employed, and all access have been removed from our applications, systems, and premises. In addition, we have contacted banking authorities and consulted with legal to seek remedies as allowed by local jurisdiction.

We have frozen affected accounts and are in the process of issuing a new account number and a replacement HSA debit card. A separate communication will be sent to you regarding the new account and replacement card. In addition, we will restore the fraudulent withdrawals to your new account. We apologize for any inconvenience this has caused. We are continuing our investigation and we shall continue to take steps designed to ensure your personal information and account is safe.

WHAT CAN YOU DO:

We are offering affected individuals free credit monitoring for one year. Enclosed is a packet with the credit monitoring service details for you to activate this service.

We recommend you regularly review and monitor all your accounts, change your security questions, and change your passwords.

You may wish to contact credit reporting agencies to request a fraud alert, credit freeze, or take other actions to monitor your credit.

Free Credit Report Information. We recommend ordering a credit report to review your accounts and credit history for any signs of unauthorized transactions or activity. U.S. residents are entitled to one free credit report annually from each of the three major credit bureaus. To order visit www.annualcreditreport.com or call (877) 322-8228.

Immediately report any unauthorized activity on your credit or bank account to your financial service providers. You have the right to file a report with your local law enforcement if you ever suspect you are the victim of identity theft or fraud. You can also file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at (877) 438-4338.

Free "Fraud Alert" or "Security Freeze" Information. We also recommend contacting the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

Equifax:
Consumer Fraud Division
P.O. Box 740256
Atlanta, GA 30374
800-685-1111
www.equifax.com/personal/credit-report-services

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
888 397-3742
www.experian.com/help

TransUnion:
TransUnion LLC
P.O. Box 2000
Chester, PA 19022-2000
888-909-8872
www.transunion.com/credit-help

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC.

Maryland Residents: You may obtain information about preventing identity theft from the FTC or the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202; Tel: (888) 743-0023; or http://www.oag.state.md.us.

North Carolina Residents: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699-9001; Tel: (919) 716-6400; Fax: (919) 716-6750; or http://www.ncdoj.com.

Rhode Island Residents: You may obtain information about preventing identity theft from the FTC or the Rhode Island Attorney General's Office at 150 South Main Street, Providence, RI 02903; Tel: (401) 274-4400; or http://www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.

FOR MORE INFORMATION:

We value your business and are sorry this situation occurred. Please contact me with any questions or concerns at fraudtransactionoperations@conduent.com .

Sincerely,

Aurela Sicard

Aurela Sicard
Specialist

EQUIFAX®

Enter your Activation Code:

Product Information

Equifax ID Patrol® provides you with the following key features:

- 3-Bureau credit file monitoring[1] and alerts of key changes to your Equifax®, TransUnion® and Experian® credit reports
- Access to your Equifax credit report
- One Equifax 3-Bureau credit report
- Wireless alerts (available online only). Data charges may apply.
- Automatic Fraud Alerts[2]. With a fraud alert, potential lenders are encouraged to take extra steps to verify your ID before extending credit (available online only).
- Credit Report Lock[3] Allows users to limit access to their Equifax credit report by third parties, with certain exceptions.
- Internet Scanning[4] Monitors suspicious web sites for your Social Security, Passport, Credit Card, Bank, and Insurance Policy Numbers, and alerts you if your private information is found there.
- Lost Wallet Assistance. If you lose your wallet, we'll help you cancel and re-issue your cards and ID
- Up to $1 MM in identity theft insurance[5]
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.

Enrollment Instructions

To sign up online for online delivery go to www.myservices.equifax.com/patrol

1. Welcome Page: Enter the Activation Code provided above in the "Activation Code" box and click the "Submit" button.

2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.

3. Create Account: Complete the form with your email address, create a User Name and Password, after reviewing the Terms of Use, check the box to accept and click the "Continue" button.

4. **Verify ID**: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.

5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features.

[1]Credit monitoring from Experian® and Transunion® will take several days to begin.

[2]The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3]Locking your Equifax credit file with Credit Report Control will prevent access to your Equifax credit file by certain third parties, such as credit grantors or other companies and agencies. Credit Report Control will not prevent access to your credit file at any other credit reporting agency, and will not prevent access to your Equifax credit file by companies like Equifax Global Consumer Solutions which provide you with access to your credit report or credit score or monitor your credit file; Federal, state and local government agencies; companies reviewing your application for employment; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; for fraud detection and prevention purposes; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[4]Internet scanning will scan for your Social Security number (if you choose to), up to 5 bank accounts, up to 6 credit/debit card numbers that you provide, up to 3 email addresses, up to 10 medical ID numbers, and up to 5 passport numbers. Internet Scanning scans thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and is constantly adding new sites to those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guaranteed that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[5] Identity theft insurance is underwritten by American Bankers Insurance Company of Florida or its affiliates. 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.