

UnitedHealthcare Privacy Office
185 Asylum Street
CT039-020A
Hartford, CT 06103



January 27, 2023

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

Submitted Via:
IDTheft@oag.state.md.us

RE: Privacy Breach Notification
 UHC File #: 543636

Mr. Karberg:

UnitedHealthcare (“UHC” or “We”) are writing to inform you of a recent incident that affected a Maryland resident.

We recently learned from our Business Associate, MultiPlan, of a security incident involving a downstream third-party vendor, Three Rivers Provider Network (“Three Rivers”).

Through our investigation, we learned that on June 3, 2022, Three Rivers identified a security incident involving unauthorized access to a single Three Rivers employee’s email account. According to Three Rivers, the unauthorized access occurred between June 2, 2022 and June 3, 2022 and involved an employee’s email account who was responsible for processing appeals and thus certain emails and their attachments in the email account contained consumer related Protected Health Information as defined in 45 C.F.R §160.103.

On January 20, 2023, after analysis of data provided by Three Rivers , UHC confirmed that one (1) Maryland resident was impacted as a result of this incident.

It is unclear whether any information belonging to the Maryland resident was actually viewed or acquired; however, the information potentially disclosed by this issue included a combination of the Maryland resident’s first and last name, address, member ID number, insurance policy number, date of birth, Social Security number, claims and health condition information as well as provider information. The issue did not involve disclosure of driver’s license number or financial account information.

To date there is no evidence to suggest that any affected individuals’ information has been misused in any way. However, it was not possible to confirm that any information viewed or acquired was destroyed and not retained or shared with others.

Written notice will be provided to the impacted Maryland resident by Three Rivers on or about January 30, 2023. The notification letter recommends steps the impacted individual can take to protect their identity, including informing them that they should report suspected incidents of identity theft to local law enforcement or the attorney general. It also explains to them how to

place a fraud alert and/or security freeze on their credit file and provides them with the contact information for the national credit reporting agencies and the Federal Trade Commission. A sample of the notice letter that that will be sent to the affected resident(s) is enclosed. Additionally, UHC is notifying other regulatory agencies as required.

Protecting the personal information of individuals is very important to us. Immediately upon learning of the issue, UHC ensured that Three Rivers had taken appropriate steps to mitigate the incident and implemented corrective actions to help prevent future incidents of similar nature from occurring in the future. This includes but is not limited to upgrading its MFA systems, updating retention policies and automatic archiving of email, implementing access control policies and procedures and using a third-party to retrain staff on privacy and security practices.

If you have any questions about this incident, please contact me directly.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Joshua Devine', is placed over a light blue rectangular background.

Joshua Devine, CIPP/US
Investigations Lead Counsel/Associate General Counsel – Privacy & Cyber, LCRA
UnitedHealthcare Corporate
O 860-702-6805
E joshua_devine@uhc.com
185 Asylum Street | CT039-020A | Hartford, CT 06103



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

December 29, 2022

i8101-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L02 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Re: **NOTICE OF DATA BREACH**

Dear Sample A. Sample:

We write to inform you that Three Rivers Provider Network (“**Three Rivers**”), a downstream vendor providing services on behalf of <Extra1> experienced a security incident that may have involved your personal information. Three Rivers contracts with healthcare providers who agree to provide care to <Extra1>’s plan participants at a discount, when those plan participants have services rendered out of network. On occasion, Three Rivers may need to receive personal information about a plan participant to effectively manage claims for services rendered.

WHAT HAPPENED? On June 3, 2022, Three Rivers identified a security matter involving unauthorized access to a Three Rivers individual’s email account between June 2, 2022 and June 3, 2022. This individual was involved in processing appeals and thus certain emails and their attachments in the email account contained plan participant information. Upon learning of the incident, Three Rivers terminated the unauthorized access by, among other things, disabling the impacted email account and resetting the email account password. An investigation supported by forensics experts was commenced to determine what happened. Three Rivers understands that during the period of unauthorized access, certain data from that email account may have been downloaded. On August 17, 2022, it was determined that this email account contained a record of an appeal with your personal information, either because the appeal was associated with your policy and/or with services you received.

WHAT INFORMATION WAS INVOLVED? Your information that may have been accessed and/or acquired includes: <extra 2>, <extra 3>, <extra 4>, <extra 5>, <extra 6>, <extra 7>, <extra 8>, <extra 9>, <extra 10>, <extra 11>, <extra 12>, and <extra 13>.

WHAT WE ARE DOING. Please know that protecting your personal information is something we take very seriously. We have taken steps to address the incident and to reduce the likelihood of a similar incident occurring in the future. While there is insufficient evidence to confirm whether your information was in fact downloaded, out of an abundance of caution we are sending you this notice and providing you with an offer of credit monitoring at no cost to you as detailed below.

WHAT YOU CAN DO. We are confident that no financial information, such as financial account information or credit card numbers, was involved in this incident. It is also always a good practice though to remain vigilant for suspicious activity and to regularly review your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity. If you identify suspicious activity, you should contact the company that maintains those respective accounts on your behalf. Sometimes, bad actors try to use schemes including “phishing” attempts in which they may pretend to represent Three Rivers or reference this incident and so remaining vigilant against schemes is also always a good practice.

0000002



i8101-L02

OTHER IMPORTANT INFORMATION. The Federal Trade Commission (“FTC”) recommends that you remain vigilant by checking your credit reports periodically. Checking your credit reports can help you spot problems and address them quickly. You can also order free copies of your annual reports through www.annualcreditreport.com. You should monitor your financial accounts for any suspicious activity. For more information about steps you can take to reduce the likelihood of identity theft or fraud, call 1-877-IDTHEFT or 1-877-438-4338, visit the FTC’s website at www.ftc.gov/bcp/edu/microsites/idtheft/ or write to: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. However, if you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state’s attorney general, or the FTC. Additional information about protecting your identity is attached to this notice.

FOR MORE INFORMATION. We sincerely regret any inconvenience this incident may cause. If you have any questions about credit monitoring, please call 855-904-2303 (Monday - Friday 9am-9pm EST, Saturday - Sunday 9am-6pm EST). If you have questions about this security matter and/or this notice, please call 855-904-2303.

Sincerely,

A handwritten signature in black ink that reads "Scott Smith". The signature is written in a cursive, flowing style.

Credit Monitoring Instructions

We have arranged for you to receive credit monitoring at no cost to you. (See enclosed instructions.) If you choose to enroll, you will receive communications detailing any key changes to your credit reports. To enroll in this service, please contact Equifax by calling the phone number listed below. If you have internet access, you may also enroll by visiting the website listed below. To enroll, you will also need the Activation Code provided below. Your coverage will last for 24 months from the date of enrollment.

Phone enrollment: +1-(866) 237-5873
Monday - Friday 9am-9pm EST
Saturday - Sunday 9am-6pm EST

Alternate website enrollment: www.equifax.com/activate
Your Activation Code: **ABCDEFGHI**
Enrollment Deadline: January 31, 2023

Contact Information for Consumer Reporting Agencies and Information on Credit Report Fraud Alerts

You may also choose to place a fraud alert on your credit file, which is free of charge to you and can be done with any **one** of the companies listed below (i.e., if you place a fraud alert with one company, they will automatically notify the others). A fraud alert tells creditors to contact you **before** they open any new accounts or change your existing accounts.

	Experian	Equifax	TransUnion
Phone	+1-(888) 397-3742	+1-(800) 525-6285 or +1-(888) 766-0008	+1-(800) 680-7289
Address	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	www.experian.com/fraud/center.html	www.equifax.com/personal/credit-report-services	fraud.transunion.com/fa/fraudAlert/landingPage.jsp

Information on Security Freezes

In addition to a fraud alert, you may place a security freeze on your credit file. A security freeze **will block** a credit bureau from releasing information from your credit report **without your prior written authorization**. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. There is no cost to place, lift or remove a security freeze.

To place a security freeze on your credit report, you may send a written request to **each** of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting **each** consumer reporting agency online. To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (State driver's license or ID card, military identification, etc.).

	Experian	Equifax	TransUnion
Address	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	www.experian.com/freeze/center.html	www.equifax.com/personal/credit-report-services	https://www.transunion.com/test/new-freeze

0000002



You may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; +1 (877) 382-4357; or www.consumer.gov/idtheft.

State-Specific Information

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. If you are a resident of the following states, the following information applies to you.

California Residents: Visit the California Office of Privacy Protection (<https://oag.ca.gov/privacy>) for additional information on protection against identity theft.

District of Columbia Residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; +1 (202) 727-3400; oag@dc.gov, and www.oag.dc.gov.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Kentucky Residents: The Attorney General can be contacted at 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: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov. Three Rivers is located at 910 Hale Pl #101, Chula Vista, CA. 91914.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: Please note that you have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, +1 (800) 771-7755; or www.ag.ny.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.



Sample A. Sample
Enter your Activation Code: **ABCDEFGHI**
Enrollment Deadline: **January 31, 2023**

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **ABCDEFGHI** then click "Submit"

1. **Register:**

Complete the form with your contact information and click "Continue".

If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.

Click "View My Product" to access the product features.

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

²Credit monitoring from Experian and TransUnion will take several days to begin.

³WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

0000002



⁵Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; 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

⁶The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.



DLA Piper LLP (US)
One Liberty Place
1650 Market Street
Suite 5000
Philadelphia, Pennsylvania
19103-7300

Ron Plesco
(215) 656-2453
Ron.Plesco@us.dlapiper.com

July 21, 2023

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Security Incident Notification

Dear Attorney General Frosh:

I am writing on behalf of Three Rivers Provider Network (“TRPN”) pursuant to Md. Code Ann., Com. Law § 14-3504, regarding an incident we previously report about.

On June 3, 2022, TRPN identified access to one (1) employee email account by an unauthorized party (the “Incident”). The internal security team immediately took steps to secure the impacted account, including changing the password to the account and removing the suspicious device from multi-factor authentication. Upon discovery, TRPN promptly launched a comprehensive investigation with the assistance of cybersecurity experts to undertake a full forensic analysis of the Incident.

TRPN’s in-depth investigation of the Incident determined that the unauthorized user gained access to the compromised account on June 2, 2022, and the last unauthorized activity in the account occurred on June 3, 2022. With the assistance of cybersecurity experts, TRPN worked diligently to analyze impacted data potentially accessed by the unauthorized user to identify potentially impacted personal information. On August 17, 2022, the results of the investigation revealed that personal information of certain TRPN clients was impacted. TRPN later determined three (3) Maryland residents were potentially impacted. On October 8, 2022, our investigation determined an additional eleven (11) Maryland individuals of TRPN clients were potentially impacted. TRPN then worked with their clients to confirm that notices should be mailed on their behalf. TRPN later determined through additional investigation that, in total, sixty-seven (67) Maryland individuals were potentially impacted by the Incident. TRPN continued to work with their clients to confirm that notices should be mailed on their behalf.

The information affected varies by individual but includes one or more of the following types of personal information: names, addresses, emails addresses, dates of birth, social security numbers, passport numbers, driver’s license numbers, health insurance numbers, and health information. It does not include credit card numbers or sensitive financial information. The notification letter sent to impacted Maryland residents will identify the specific data elements impacted for each individual receiving notice.

TRPN has implemented additional security measures to prevent this activity from occurring in the future including, but not limited to, creating new conditional access rules to prevent access from unauthorized IP addresses; implementing new monitoring and alert rules to detect access from first time IP addresses and improbable travel scenarios; and updating MFA protocols. Please note that TRPN has reviewed their Microsoft Office 365 email

environment for indications of unauthorized access to any other TRPN email accounts. The investigation did not identify any additional TRPN email accounts with indications of unauthorized access. TRPN continues to monitor the Internet for potential misuses of Maryland residents' data, and there is no indication to suggest the impacted data is being misused.

On October 15, 2022, TRPN began mailing notifications to the affected Maryland residents, and continued to do so on a rolling basis over the coming months as additional individuals were identified, offering a 24-month subscription for credit monitoring and identity protection through Equifax Complete Premier Credit Monitoring and Identity Theft protection. Affected residents may enroll in the services at no cost by using a promotional code and instructions provided to them in the notification letter.

A sample notification letter is enclosed.

Should you have any questions regarding this matter or if we can be of any further assistance to the Maryland residents affected by this Incident, please contact me at Ron.Plesco@us.dlapiper.com.

Respectfully submitted,

A handwritten signature in blue ink, appearing to read "Ron Plesco".

Ron Plesco
Partner
DLA Piper LLP

Enclosure: Sample Notification Letter



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 15, 2022

i4752-L02-0000002 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L02 GENERAL
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



Re: NOTICE OF DATA BREACH

Dear Sample A. Sample:

On behalf of Three Rivers Provider Network (“TRPN”), we write to inform you of an incident that may have involved personal information about you. We deeply regret that this incident occurred and take seriously the security of personal information.

WHAT HAPPENED? On June 3, 2022, TRPN identified unauthorized access to one (1) employee email account by an unauthorized party. We immediately initiated an investigation and secured the compromised account. On August 17, 2022, we discovered that your personal information may have been accessed by the unauthorized party.

WHAT INFORMATION WAS INVOLVED? Personal information that may be affected includes your name, address, date of birth, social security number, treatment or diagnosis information, prescription information, provider name, MRN or patient ID number, Medicare or Medicaid number, health insurance information, health insurance policy number, or treatment cost information.

WHAT WE ARE DOING. We have thoroughly investigated this incident and taken additional steps to secure our systems. Please know that protecting your personal information is something that we take very seriously, and we value your trust in doing business with us. We apologize for both this unfortunate incident and any inconvenience it may cause you. We have taken steps to address the incident and ensure that this does not occur in the future. We are providing notice and offering credit monitoring services to individuals based on the personal information that was potentially impacted.

WHAT YOU CAN DO. We are confident that no financial information, such as financial account information or credit card numbers was involved in this incident. You should be on guard for schemes, known as phishing attacks, where malicious actors may pretend to represent TRPN or reference this incident. If you have questions, please contact us at the number described below. To help protect your identity, we are offering **complimentary** credit monitoring services as described below. This helps detect possible misuse of your personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft.

OTHER IMPORTANT INFORMATION. The Federal Trade Commission (FTC) recommends that you remain vigilant by checking your credit reports periodically. Checking your credit reports can help you spot problems and address them quickly. You can also order free copies of your annual reports through www.annualcreditreport.com. You should monitor your financial accounts for any suspicious activity. For more information about steps you can take to reduce the likelihood of identity theft or fraud, call 1-877-IDTHEFT or 1-877-438-4338, visit the FTC’s website at www.ftc.gov/bcp/edu/microsites/idtheft/ or write to: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. However, if you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state’s attorney general, or the FTC.

0000002



i4752-L02

Credit Monitoring Instructions

We have arranged for you to receive free credit monitoring to help you protect your identity and credit information. (See enclosed instructions.) If you choose to enroll, you will receive communications detailing any key changes to your credit reports. To enroll in this service, please contact Equifax by calling the phone number listed below. If you have internet access, you may also enroll by visiting the website listed below. To enroll, you will also need the Activation Code provided below. Your coverage will last for 24 months from the date of enrollment.

Enrollment URL: www.equifax.com/activate
Your Activation Code: **ABCDEFGHI**
Enrollment Deadline: **January 31, 2023**

Contact Information for Consumer Reporting Agencies and Information on Credit Report Fraud Alerts

You may also choose to place a fraud alert on your credit file, which is free of charge to you and can be done with any *one* of the companies listed below (i.e., if you place a fraud alert with one company, they will automatically notify the others). A fraud alert tells creditors to contact you *before* they open any new accounts or change your existing accounts.

	Experian	Equifax	TransUnion
Phone	1-888-397-3742	1-800-525-6285 or 1-888-766-0008	1-800-680-7289
Address	Experian Fraud Division P.O. Box 9554 Allen, TX 75013	Equifax Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Credit Report Fraud Alert Form	www.experian.com/fraud/ center.html	www.equifax.com/personal/ credit-report-services	fraud.transunion.com/fa/ fraudAlert/landingPage.jsp

Information on Security Freezes

In addition to a fraud alert, you may place a security freeze on your credit file. A security freeze *will block* a credit bureau from releasing information from your credit report *without your prior written authorization*. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. There is no cost to place, lift or remove a security freeze.

To place a security freeze on your credit report, you may send a written request to each of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting each consumer reporting agency online. Please provide the information requested, which varies by consumer reporting agency, but typically includes: full name, address, Social Security number, date of birth, proof of identity and proof of address.

	Experian	Equifax	TransUnion
Address	Experian Security Freeze P.O. Box 9554 Allen, TX 75013	Equifax Security Freeze P.O. Box 105788 Atlanta, Georgia 30348	TransUnion LLC P.O. Box 2000 Chester, PA 19016
Online Security Freeze Form	www.experian.com/freeze/ center.html	www.equifax.com/personal/ credit-report-services	www.transunion.com/test/new- freeze

You may obtain information from the FTC and the credit reporting agencies about fraud alerts and security freezes.

FOR MORE INFORMATION. If you have questions about the data breach, please call 855-904-2303 (Monday - Friday 9am-5pm EST). We sincerely regret that this incident occurred.

Sincerely,



State-Specific Information

If you are a resident of the following states, the following information applies to you.

For residents of Maryland, New York, North Carolina, Rhode Island, the District of Columbia: For information on how to avoid identity theft or to contact your state's attorney general, please use the below information.

Maryland Attorney General	North Carolina Attorney General	Rhode Island Attorney General
1-888-743-0023 www.oag.state.md.us Attorney General of Maryland 200 St. Paul Place Baltimore, MD 21202	1-877-566-7226 www.ncdoj.gov Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001	1-401-274-4400 www.riag.ri.gov Rhode Island Office of the Attorney General 150 South Main Street Providence, RI 02903
District of Columbia Attorney General	New York Attorney General	
1-202-727-3400 www.oag.dc.gov Office of the Attorney General for the District of Columbia 441 4th St. NW Washington, DC 20001	1-800-771-7755 www.ag.ny.gov Office of the Attorney General The Capitol Albany, NY 12224-0341	

For residents of New Mexico: You have rights under the federal Fair Credit Reporting Act (FCRA). These include: the right to access information in your consumer file at a consumer reporting agency; to dispute incomplete or inaccurate information in your consumer file at a consumer reporting agency; to have consumer reporting agencies correct or delete inaccurate information in your consumer file; the right to block information in your consumer file that is the result of identity theft; and the right to have a fraud alert placed on your consumer file (as described above). For more information, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

For residents of Rhode Island: Under Rhode Island law, you have the right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.





Sample A. Sample
Enter your Activation Code: ABCDEFGHI
Enrollment Deadline: **January 31, 2023**

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code of **ABCDEFGHI** then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹ The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

² Credit monitoring from Experian and TransUnion will take several days to begin.

³ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

⁴ The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; 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

⁶ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.