



Return to Mail Processing Vendor:

<Return Address>

<City> <State> <Zip>

Via First-Class Mail

<<Name 1>>

<<Name 2>>

<<Business Name>>

<<Address 1>>

<<Address 2>>

<<City>>, <<State>> <<Zip>>

<<MAILDATE>>

<<Variable Header>>

Dear <<Name 1>>:

Hutchison Whitehead, LLC, which <<Variable Data 1>><<Variable Data 2>>, recently experienced a data security incident that may have affected your personal information. Based on what we currently know, we have no indication that your personal information has been used to commit fraud or identity theft. We wanted to make sure, however, that you are aware of the incident, the protective measures we have taken in response, and to provide details on the steps you can take – should you deem it appropriate further to protect your information. We take your security and privacy seriously and accordingly, have taken steps since the incident to prevent a recurrence and protect you. <<Variable Data 4>>

What Happened

On or about September 11, 2023, Hutchison Whitehead experienced a ransomware incident. During a typical ransomware incident, cybercriminals try to encrypt or “lock” an organization’s digital files in an attempt to get paid for a digital key to unlock the files. We promptly launched an investigation, engaged a national cybersecurity firm to assist in assessing the scope of the incident and took steps to mitigate the potential impact on clients and others whom we serve. Unfortunately, these types of incidents are becoming increasingly common and even organizations with some of the most sophisticated IT infrastructure available are affected. We have worked diligently to determine what happened and what information was involved as a result of this incident. The third-party forensic investigation determined the incident occurred between September 11 and September 12, 2023.

What Information Was Involved

The elements of your personal information that may have been impacted may have included your <<Variable Data 3>>, together with your name and address. To repeat, we have no indication that your personal information has been used to commit fraud or identity theft.

What We Are Doing

We take this incident very seriously and have strengthened our systems' security to reduce the likelihood of a similar event in the future. In addition, out of an abundance of caution, we have arranged for you to activate, at no cost to you, free of charge, enrollment for two years in a Complete Premier package of services from Equifax. This package includes credit monitoring, a credit report, credit score and identity fraud protective services that provide proactive antifraud assistance and remediation to help with any questions that you might have or in the event that you become a victim of fraud.

What You Can Do

While we have no indication that fraud has occurred due to this incident, data frauds are not uncommon. We therefore recommend that you review the next few pages, which contain important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes on your personal credit.

To enroll in the complimentary services we are offering you, please follow these steps:

- ☐ Ensure that you enroll by <<Enrollment Deadline>> or the code will be inactive.
- ☐ Go to www.equifax.com/activate
- ☐ Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow the instructions to register, create an account and verify your identity.
- ☐ Upon verification of identity, you will see the Checkout Page. Click "Sign Me Up" to finish enrolling.
- ☐ The confirmation page shows your completed enrollment. Click "View My Product" to access the features.

In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The service will not affect your credit score. To activate monitoring services, you will need an e-mail account as well as an Internet connection. You may also be required to provide your name, date of birth, and Social Security number to confirm your identity. Under privacy laws, we cannot register you directly. Certain services might be unavailable to individuals without a credit file at the credit bureaus or an address in the United States (or its territories) and a valid Social Security number.

For More Information

We regret any inconvenience or concern this incident may cause. Protecting your personal information is our top priority. If you have questions, please call 888-722-8147, M-F, 9:00am – 9:00pm Eastern Standard Time.

Sincerely,

Michael Whitehead

Michael Whitehead, Principal
Hutchison Whitehead, LLC

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.

Implementing an Identity Protection PIN (IP PIN) with the IRS:

To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>. If you wish to get an IP PIN and you don't already have an account on IRS.gov, you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.
- A new IP PIN is generated each year for your account.
- Logging back into the Get an IP PIN tool, will display your current IP PIN.
- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Vermont: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For Residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

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

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.