MAYER | BROWN

CONFIDENTIAL TREATMENT REQUESTED

VIA EMAIL

February 4, 2025

Mayer Brown LLP
1999 K Street, N.W.
Washington, DC 20006-1101
United States of America

T: +1 212 506 2500
F: +1 212 262 1910

mayerbrown.com

Amber Thomson
Partner

Attorney General John M. Formella
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
attorneygeneral@doj.nh.gov

Re: Hewlett Packard Enterprise Company – Notice of Data Event

Dear Attorney General Formella:

We represent Hewlett Packard Enterprise Company ("HPE"). We are writing to notify your office of a recent event that may affect the security of certain personal information relating to 6 New Hampshire residents. Please note that we may supplement this notice with facts learned after its submission and that by providing this notice, HPE does not waive any rights or defenses, including regarding the applicability of New Hampshire law, the applicability of the New Hampshire data breach notification statute, or personal jurisdiction.

On December 12, 2023, HPE was notified that a suspected nation-state actor had gained unauthorized access to HPE's cloud-based email environment. With assistance from external cybersecurity experts, HPE immediately responded to investigate, contain, and remediate the incident, eradicating the activity. Please note that the incident has since been contained and remediated.

HPE's forensic investigation determined that certain individuals' personal information may have been subject to unauthorized access. With the assistance of e-discovery specialists, HPE conducted a thorough review of the data at issue to identify the types of information that may have been subject to unauthorized access and determine to whom this information relates.

On January 29, 2025, HPE began providing notice of this event to impacted individuals, in accordance with applicable law. Notice is being provided in substantially the same form as the letter attached hereto as Exhibit A.

HPE takes this incident and the security of information in its care seriously. In addition to the guidance and information provided in the written notice, HPE is offering impacted individuals access to of complimentary credit monitoring and identity theft restoration services.

Should you have any questions about this notification or require further information, please do not hesitate to contact me.

Sincerely,

Amber Thomson
Partner

Enclosures: Consumer Notification Letter

Privileged & Confidential
Draft for Discussion

Individual Notice Letter

[Letterhead]

[Date], 2025

[Recipient Address]

Re: **Notice of Data Breach**

Dear [Individual name]:

We are writing to inform you of a cybersecurity incident that may have impacted your personal information. We are contacting you to explain the circumstances of the incident, the types of information involved, and protective measures you can take, should you deem it appropriate to do so.

What Happened?

On December 12, 2023, Hewlett Packard Enterprise Company ("HPE") was notified that a suspected nation-state actor had gained unauthorized access to our cloud-based email environment. With assistance from external cybersecurity experts, HPE immediately responded to investigate, contain, and remediate the incident, eradicating the activity.

Our forensic investigation determined that certain individuals' personal information may have been subject to unauthorized access. With the assistance of e-discovery specialists, HPE conducted a thorough review of the data at issue to identify the types of information that may have been subject to unauthorized access and determine to whom this information relates.

What Personal Information Was Involved?

The investigation determined that the following types of your personal information may have been involved: your

What Are We Doing?

HPE takes this incident and the security of information in our care seriously. In response to this incident, we have taken steps to contain and remediate the incident. Additionally, we have notified law enforcement. Moreover, we took additional remediation actions, such as strengthening network security by rotating passwords, tokens and keys, expanding of monitoring and logging measures, additional controls and requirements for privileged account logins, and expanding internal communication around security measures.

What You Can Do.

Considering the nature of the incident and of the affected personal information, we cannot rule out that there may be attempts to carry out fraudulent activity. For this reason, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your financial account statements and credit reports for any anomalies. We also encourage you to review the enclosed *Steps You Can Take to Help Protect Your Personal Information* for additional guidance.

To protect you from potential misuse of your information, we are offering a complimentary [X] membership in Equifax® Complete Premier. Equifax® Complete Premier is completely free to you and enrolling in this program will not hurt your credit score.

Enter your Activation Code: *<<Activation Code>>*
Enrollment Deadline: *<<Enrollment Deadline>>*

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 VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] 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 alerts,[4] which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]

---

[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

- 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 theft[6]
- 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 <<*Activation Code*>> 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.

In addition to enrolling in credit monitoring, we recommend that you remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Protect Your Personal Information* for additional guidance.

For More Information.

If you have questions regarding this incident, please call [call center telephone number] Monday through Friday from [time frame], or Saturday and Sunday from [time frame].

We take the protection of your information seriously and sincerely regret any inconvenience this incident may cause you.

---

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.

Privileged & Confidential
Draft for Discussion

Sincerely,

HPE

Privileged & Confidential
Draft for Discussion

Steps You Can Take to Protect Your Personal Information

We encourage you to remain vigilant to signs you may be the victim of identity theft and to consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize and notify the credit bureaus as soon as possible in the event there are any.

Place a Fraud Alert on Your Credit or Consumer File: To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit or Consumer File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com

TransUnion Fraud Victim Assistance Division www.transunion.com
P.O. Box 2000
Chester, Pennsylvania 19016

The consumer reporting agencies may require that you provide proper identification prior to honoring your request. In order 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, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft.

Placing a security freeze on your file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe your identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

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

For District of Columbia Residents: You can obtain information from the FTC and the Office

of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at: 441 4th Street, NW, Washington, DC 200001, 202-727-3400, www.oag.dc.gov.

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

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us.

For New Mexico Residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7226 (Toll-free within North Carolina), 919-716-6000, www.ncdoj.gov.

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

For Rhode Island Residents: You can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-

4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.