2024-496

BROWN

Office of Information Technology
Box 1885
Providence, RI 02912

NOTICE OF DATA BREACH

Dear [NAME]:

We are writing to inform you about a recent security incident involving unauthorized access to certain personal information within Brown University's services. The privacy and security of our community members are of utmost importance to us, and we deeply regret any inconvenience or concern this may cause you.

What Happened?

On or about January 16, 2024, we discovered suspicious activity within Workday. We immediately launched a thorough investigation to determine the nature and scope of the incident. Through the investigation, we confirmed that your credentials appear to have been compromised by a successful phishing campaign and access to Workday was ultimately granted through a fraudulent two-step authorization request, resulting in an unauthorized individual or group gaining access to your individual information in Workday.

What Information was Involved?

The breach potentially exposed your personal information, including but not limited to direct deposit banking information.

What We are Doing.

We take this incident and the security of information in our care seriously. Upon learning about this incident, we promptly took steps to confirm the security of our systems and notify potentially affected individuals. We are also reporting to regulatory officials, as required. Brown has reissued any redirected direct deposit funds to your original bank. While we had policies and procedures in place at the time of the incident regarding security of information, we are reviewing those existing policies and procedures to further protect against similar incidents moving forward. We have actively increased the communication with our community about the risk of credential loss through phishing and dangers of responding to unexpected two-step authorization requests.

While we are unaware of any identity theft or fraud because of this incident, as an additional precaution, we will be offering you complimentary identity monitoring services through a third-party provider.

Details of this offer and instructions on how to activate these services will follow in a separate communication.

What You Can Do.

- You may enroll in the free credit monitoring service we will be offering in response to this incident.
- Please also review how to Spot, Protect Yourself, and Recovery from Phishing and information about Two-Step Verification
- Monitor Your Accounts:
    - Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, tollfree, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.
    - Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.
    - As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:
        1. Full name (including middle initial as well as Jr., Sr., 11, III, etc.);
        2. Social Security number;
        3. Date of birth;
        4. Addresses for the prior two to 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, etc.); and
        7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.
    - Should you wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	Transunion

https:/ /www.equifax.com/personal/credit-report-services/	https://www.experian.com/help /	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	Trans Union Credit Freeze, P.O. Box 160, Woodlvn, PA 19094

- Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: l-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement. The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies.

If you have any questions or require further information, please do not hesitate to contact Brown's IT Service Center at 401-863-4357 or email us at ithelp@brown.edu.

Thank you for your understanding and cooperation.

Sincerely,

Mark Dieterich
Chief Information Security Officer
Brown University