

[REDACTED]

From: Harding, Jennifer T <jennifer_harding@harvard.edu>
Sent: Friday, January 15, 2021 9:31 AM
To: DOJ: Consumer Protection Bureau <DOJ-CPB@doj.nh.gov>
Subject: HBS: New Hampshire AG Notification

EXTERNAL: Do not open attachments or click on links unless you recognize and trust the sender.

Attorney General Gordon MacDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Incident

Dear Attorney General Gordon MacDonald,

We write to inform you about a recent data security incident that impacted files containing the personal information of three of your state's residents.

On December 29, 2020, Harvard Business School (HBS) was notified by one of its software vendors that the vendor had identified an anomaly in the vendor's software. HBS promptly launched an investigation and determined that files stored on the system provided by the vendor were downloaded by an unauthorized actor within the December 21-23 timeframe. Some of the files contained personal information including names, contact information, social security numbers, financial information, credit card information, government identification, date of birth, educational information or health information.

HBS has worked with the vendor to resolve the vulnerability in the software and has not observed any suspicious activity since those dates. HBS is also coordinating with local and federal law enforcement to further its investigation into the incident. The vendor has taken additional measures in response to the incident, changing their anomaly detection system to run more frequently as well as making other security enhancements.

The security, confidentiality and integrity of personal information at HBS is protected by a

comprehensive written information security program. In addition, HBS has in place reasonable and appropriate technical and operational measures to protect personal information. HBS patches the vendor's software weekly, has the vendor monitor the system, and monitors its networks for signs of any malicious activity.

HBS is sending the enclosed notification letter, by mail, to three New Hampshire individuals whose personal information was present on the files downloaded by the unauthorized actor. In addition, as reflected in the letter, each notified individual is being offered 24 months of Experian's® IdentityWorksSM identity protection services at no cost. HBS is also notifying additional individuals on a voluntary basis.

If you have any questions about this event, please contact me at 617-496-4192 or jennifer_harding@harvard.edu.

Sincerely,

/s/ Jennifer Harding

Jennifer T. Harding
Office of the General Counsel – Harvard University
Smith Campus Center
1350 Massachusetts Avenue
Cambridge, MA 02138
(617) 496 -4192



HARVARD | BUSINESS | SCHOOL

CHRISTOPHER PRINGLE

INFORMATION SECURITY OFFICER AND
MANAGING DIRECTOR OF IT COMPLIANCE

January 11, 2021

Name

Address1

City State Postal Code

Dear Name,

We are writing to inform you about a recent security incident that involved files containing your personal information and to provide you with an offer for free credit monitoring and a way to contact us if you would like additional information.

WHAT HAPPENED

On December 29, 2020, Harvard Business School (HBS) was notified by one of its software vendors of unauthorized access to HBS files as the result of a vulnerability in the vendor's software. Our investigation has determined that at least one file containing your personal information was downloaded by an unauthorized actor within the December 21-23 timeframe.

HBS has worked with the vendor to resolve the vulnerability in the software and we have not observed any suspicious activity since those dates.

WHAT INFORMATION WAS INVOLVED

The downloaded files contained personal information about you including: [here we include data categories customized for each individual]

WHAT WE ARE DOING

We take the confidentiality and security of personal information very seriously. HBS promptly applied a patch supplied by the vendor to resolve the vulnerability in the vendor's software and has not seen any related suspicious network activity since that date. HBS is coordinating with local and federal law enforcement to further investigate the incident. In addition to patching the vulnerability, the vendor has changed its anomaly detection routine, which helped it identify this activity, to run more frequently and has made other security enhancements.

WHAT YOU CAN DO

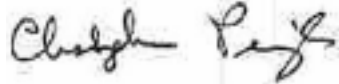
It is always advisable to remain alert for possible fraud and identity theft by reviewing and monitoring your credit and financial account information for unauthorized activity. The enclosed "General Information About Identity Theft Protection" provides further information about steps that individuals can take. Federal regulatory agencies recommend vigilance for the next 12 to 24 months and that you report any suspected incidents of fraud to the relevant financial institution.

We are providing you with a two-year membership in Experian's® IdentityWorksSM monitoring product¹ at no cost to you. Details about this offer and your activation code are included in the enclosed "Details Regarding 24-Month Experian IdentityWorks Membership." If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332.

FOR MORE INFORMATION

Please email [XXXX](#) or contact us at XXX-XXX-XXXX if you have any questions related to this letter.

Sincerely,

A handwritten signature in black ink, appearing to read "Christopher Pringle". The signature is written in a cursive style with a large initial "C".

Christopher Pringle

Enclosures

¹ The opportunity to subscribe to these services is not intended to suggest that you are at substantial risk of harm.

DETAILS REGARDING 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

The complimentary membership in Experian's® IdentityWorksSM provides you with identity detection and resolution of identity theft services. To activate this membership for monitoring your personal information please follow the steps below:

- Ensure that you enroll by April 30, 2021 (your code will not work after this date)
- Visit the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bplus>
- Provide your activation code: **Code**
- Provide your Engagement #: B008379

A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.¹
- **Credit Monitoring:** Actively monitors Experian, Equifax, and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms, and bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance²:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there is fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877-890-9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for two years from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

GENERAL INFORMATION ABOUT IDENTITY THEFT PROTECTION

It is always advisable to regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online (www.annualcreditreport.com), by calling toll free (877.322.8228), or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below:

- **Equifax:** P.O. Box 740241, Atlanta, GA 30374-0241 | 800.685.1111 | www.equifax.com
- **Experian:** P.O. Box 9532, Allen, TX 75013 | 888.397.3742 | www.experian.com
- **TransUnion:** 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016 | 800.916.8800 | www.transunion.com

Fraud Alert: You may contact the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

- **Equifax:** (Report Fraud) 800.685.1111
- **Experian:** (Report Fraud) 888.397.3742
- **TransUnion:** (Report Fraud) 800.680.7289

Security Freeze for Credit Reporting Agencies: You may request a security freeze on your credit reports. 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. It is free to place, lift or remove a security freeze. You must separately place a security freeze on your credit report at each credit bureau. To do so, you must contact the credit bureaus by phone, mail, or secure electronic means:

- **Equifax:** P.O. Box 105788, Atlanta, GA 30348 | 800.349.9960 | www.Equifax.com
- **Experian:** P.O. Box 9554, Allen, TX 75013 | 888.397.3742 | www.Experian.com
- **TransUnion:** P.O. Box 2000, Chester, PA 19106 | 888.909.8872 | www.TransUnion.com

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.)
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

If you request a freeze online or by phone, the agency must place the freeze within one business day. The credit bureaus have three business days after receiving a request by mail to place a security freeze on your credit report, and they must also send confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must contact the credit reporting agencies and include (1) proper identification; (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available.

You also 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 www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Steps You Can Take if You Are a Victim of Identity Theft

- **File a police report.** Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- **Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf
- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is helpful to log conversations with creditors, law enforcement officials, and other relevant parties.

Additional Steps to Avoid Identity Theft: The FTC has further information about steps to take to avoid identity theft at: <http://www.ftc.gov/idtheft>; calling 877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

State Specific Information

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164, or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, calling the Identity Theft Unit at 410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

New Mexico residents have the right to obtain a police report and request a security freeze as described above and you have rights under the Fair Credit Reporting Act as described above.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <https://ncdoj.gov/protecting-consumers/identity-theft/>, calling 919.716.6400, or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached by visiting the website at www.doj.state.or.us, calling (503) 378-4400, or requesting more information from the Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.

Rhode Island residents have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General at 410.274.4400 or 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <https://ago.vermont.gov/>.