

July 6, 2022

**To:** Office of the Attorney General  
Security Breach Notification  
200 St. Paul Place, 25 Floor  
Baltimore, MD 21202  
E-Mail: idtheft@oag.state.md.us

**From:** David Sherry, Chief Information Security Officer

**Re:** Notification of Data Exposure

---

We are writing to notify your office of a data exposure that may have affected the security of some personal information relating to 328 Maryland residents. By providing this Notice, Princeton does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

#### **Description of the Incident and Data Potentially Impacted**

On June 6, 2022, Princeton's Office of Information Technology ("OIT") discovered that certain information about some former Princeton students was accessible in electronic files publicly available on a website operated by Princeton. The files that were publicly available included social security numbers and dates of birth. Not every affected state resident had the same information exposed. The University took immediate action, including removing the information from public access and engaging a third party cybersecurity firm to investigate and assist in remediating the exposure.

Based on the investigation, there is no evidence of unauthorized access to the files through Princeton's computing systems. However, it appears that the files were accessed by third parties through the public internet. On June 10, the Office of the General Counsel became aware that the exposure may have impacted 328 residents of Maryland.

#### **Notice to Maryland Residents**

In accordance with Maryland law, Princeton intends to provide notice to all impacted Maryland residents. Written notice is being provided in substantially the same manner as the letter attached as Exhibit A.

#### **Other Steps Being Taken To Protect Maryland Residents**

Princeton University takes this exposure extremely seriously and is actively working to protect the interests of impacted individuals. In addition to the steps referenced above, Princeton is in the process of notifying affected individuals and establishing a toll free number for Maryland residents. Further, to help relieve concerns and restore confidence following this incident, we have

engaged the services of Kroll, a leading cybersecurity risk mitigation and response company, to provide identity monitoring to affected Maryland residents for two (2) years, at Princeton's expense. These identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

#### **Contact Information**

Princeton is actively monitoring the status of this situation as it develops. Should you need to contact Princeton for any reason, please contact me at (609) 258-3565 or [david.sherry@princeton.edu](mailto:david.sherry@princeton.edu).

Sincerely,



David Sherry  
Chief Information Security Officer  
Princeton University

# **EXHIBIT A**

<<FirstName>><<MiddleName>><<LastName>>

<<Date>> (Format: Month Day, Year)

<<Address1>>

<<Address2>>

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

## **Notice of Data Breach**

Dear <<FirstName>><<MiddleName>><<LastName>>,

We are writing to tell you about a data security incident that has exposed some of your personal information. Princeton University takes the protection and proper use of your information very seriously. For this reason, we are contacting you directly to explain the circumstances of the exposure.

### **What happened?**

On June 6, 2022, Princeton University's Office of Information Technology discovered that certain information about some former Princeton students was accessible in electronic files publicly available on a website operated by Princeton. The investigation into the incident suggests that this information was first made publicly available on April 28, 2020. Princeton took immediate action, including removing the information from public access and engaging a third party cybersecurity firm to investigate and assist in remediating the exposure. Based on the investigation, there was no evidence of unauthorized access to the files through Princeton's computing systems. However, it appears that the files were accessed by third parties through the public internet.

### **What information was involved?**

The information involved personal information relating to purchases of computers through Princeton University's Student Computing Initiative, including social security number and [date of birth].

### **What we are doing.**

Upon discovery of the exposure, Princeton immediately ensured that the files at issue were made inaccessible to the public. Further, Princeton completed a scan of its systems to ensure that no additional files containing personally identifiable information were publicly available. Additionally, Princeton retained a third party cybersecurity firm to independently investigate the exposure and provide advice regarding remediation and prevention.

Although we do not know that your personal information was read, copied or downloaded by any unauthorized parties, we recommend that you take steps to protect your identity. To help you do so, Princeton has engaged the services of Kroll, a leading cybersecurity risk mitigation and response company, to provide identity monitoring for two years at Princeton's expense. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

Information describing your services is included with this letter.

### **What you can do.**

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade

Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

**For more information.**

If you have questions, please call 1-???-???-????, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time. Please have your membership number ready.

Protecting your information is important to us. We are offering the services to demonstrate to you our continued commitment to your security.

Sincerely,

David Sherry

Chief Information Security Officer

Princeton University

## ADDITIONAL RESOURCES

### Contact information for the three nationwide credit reporting agencies:

**Equifax**, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

**Experian**, PO Box 2104, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

**TransUnion**, PO Box 2000, Chester, PA 119016, [www.transunion.com](http://www.transunion.com), 1-800-888-4213

**Free Credit Report.** It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit [www.annualcreditreport.com](http://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 from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Fraud Alerts.** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Security Freeze.** You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

**Federal Trade Commission and State Attorneys General Offices.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT (438-4338).

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-877-566-7226.

**For New York residents:** The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

**For Connecticut residents:** You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag).

**For Massachusetts residents:** You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html)

**For Rhode Island residents:** You may contact the Rhode Island Office of the Attorney General at (401) 274-4400, <https://riag.ri.gov/about-our-office/contact-us>.

**For the District of Columbia residents:** You may contact the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202) 727-3400, <https://oag.dc.gov/about-oag/contact-us>.

#### **Reporting of identity theft and obtaining a police report.**

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.



#### **TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES**

You have been provided with access to the following services from Kroll:

##### **Single Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

##### **Web Watcher**

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

##### **Public Persona**

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

##### **Quick Cash Scan**

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

## **\$1 Million Identity Fraud Loss Reimbursement**

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

## **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

## **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.