

COLUMBIA UNIVERSITY
IN THE CITY OF NEW YORK

August 7, 2025

By U.S. Mail

RI Office of the Attorney General
150 S. Main St.
Providence, RI 02903

To Whom It May Concern:

Columbia University ("Columbia") is providing this notice of a cybersecurity event to your office. Columbia is an educational institution based in New York.

On June 24, 2025, Columbia experienced a technical outage that disrupted certain of its IT systems. Columbia promptly activated its incident response protocols to restore affected systems, notified law enforcement, and launched an investigation. This investigation determined that, on or about May 16, 2025, an unauthorized third party gained access to Columbia's network through a publicly-exposed system. Leveraging this access, the unauthorized third party was then able to access and remove personal information from Columbia's student admissions, financial aid, and certain employee databases.

Columbia believes that the unauthorized third party obtained information provided by or related to an individual's application to Columbia, including: name, contact information, gender, ethnicity, citizenship status, test scores, academic grades, admission decision, expected graduation date, financial aid status, financial aid award, and tuition information. On July 8, 2025, Columbia determined that the affected information included Social Security numbers and dates of birth of approximately 2,524 Rhode Island residents. Columbia has not received any confirmed reports of this personal information being used for fraud or identity theft purposes. Columbia has also not identified any evidence at this time that this data has been offered for sale or otherwise posted publicly.

Columbia began sending formal notification to the affected individuals via U.S. mail on August 7, 2025. Attached is a copy of the notification template mailed to the affected individuals in your state. Columbia is providing affected individuals with 24 months of complimentary credit monitoring and identity theft protection services through Kroll. Columbia has also established a dedicated call center to answer individuals' questions.

Columbia has taken, and will continue to take, proactive measure to protect its systems and data. Specifically, upon discovering the incident, Columbia identified and blocked the unauthorized actor's access to the network and took certain ports offline to prevent further unauthorized access. Columbia has also reset passwords for any known compromised accounts and deployed additional endpoint detection and response tools to identify any suspicious activity.

If you have any questions, please contact me at fbr@gc.columbia.edu.

Regards,

Felice Rosan
General Counsel
Columbia University

Enclosure

<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>



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

<<b2b_text_1 (Notice of Data Breach/Notice of Security Incident)>>

Dear <<first_name>>:

As we previously disclosed, Columbia University recently experienced a cyber incident. We are writing to inform you of how it may impact you and your personal information, what measures we are taking and what steps you can take to protect yourself. We are providing you with information about the incident, our response, and additional measures you can take to help protect yourself.

What Happened?

On June 24, 2025, we experienced a technical outage that disrupted certain of our IT systems. We promptly activated our response process, launched an investigation with the support of external cybersecurity experts, and reported the incident to law enforcement. Our investigation determined that, on or about May 16, 2025, an unauthorized third-party gained access to Columbia's network and subsequently took certain files from our system. To date, we have no evidence that any Columbia University Irving Medical Center patient records were affected.

What Information Was Involved?

The affected data included your name, date of birth, and Social Security number, as well as any personal information that you provided in connection with your application to Columbia, or that we collected during your studies if you enrolled. This included your contact details, demographic information, academic history, financial aid-related information, and any insurance-related information and health information that you shared with us.

What We Are Doing.

We have implemented a number of safeguards across our systems to enhance our security. Moving forward, we will be examining what additional steps we can take and additional safeguards we can implement to prevent something like this from happening again.

While we are not aware of identity theft or fraud related to this incident, we are offering you two years of complimentary credit monitoring and identity restoration services through Kroll. Details about this offer and instructions on how to activate these services are enclosed with this letter. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

What You Can Do.

We understand and regret any concern this incident may cause. We encourage you to remain vigilant and review your account statements and free credit reports regularly to ensure there is no unauthorized or unexplained activity. We also encourage you to enroll in the complimentary credit monitoring services that we are offering. Please review the enclosed *Steps You Can Take to Help Protect Personal Information*, which contains details about this offer and general guidance on what you can do to safeguard against possible future misuse of your information.

For More Information.

We have established a dedicated call center to answer questions about this incident. If you have any questions regarding this incident, please call (866) 819-7006, 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding major U.S. holidays.

Sincerely,

Columbia University

Steps You Can Take to Help Protect Personal Information

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 1-877-322-8228 toll-free. 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" at no charge 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., II, 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; (4) a legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and (6) 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 consumers 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/credithelp
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Information Services LLC, P.O. Box 105069, Atlanta, GA 30348	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	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the three major credit reporting bureaus, the Federal Trade Commission, or your 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: 1-866-653-4261. 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.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Iowa residents, you are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov>. Columbia University can be reached by mail at 412 Low Memorial Library, Mail Code 4308, 535 West 116th Street, New York, NY 10027.

For Massachusetts residents, under Massachusetts law, individuals have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and <https://ag.ny.gov>. The New York Department of State Division of Consumer Protection may be contacted at: <http://www.dos.ny.gov/consumerprotection> or (800) 697-1220.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

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

For Rhode Island residents, 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. There are approximately 2,510 Rhode Island residents that may be impacted by this event.