

CLEARY GOTTlieb STEEN & HAMILTON LLP

One Liberty Plaza
New York, NY 10006-1470

T: +1 212 225 2000

F: +1 212 225 3999

clearygottlieb.com

AMERICAS	ASIA	EUROPE & MIDDLE EAST	
NEW YORK	BEIJING	ABU DHABI	LONDON
SAN FRANCISCO	HONG KONG	BRUSSELS	MILAN
SÃO PAULO	SEOUL	COLOGNE	PARIS
SILICON VALLEY		FRANKFURT	ROME
WASHINGTON, D.C.			

CRAIG B. BROD
RICHARD J. COOPER
JEFFREY S. LEWIS
PAUL J. SHIM
STEVEN L. WILNER
DAVID C. LOPEZ
MICHAEL A. GERSTENZANG
LEV L. DASSIN
DAVID H. BOTTER
JORGE U. JUANTORENA
DAVID LEINWAND
JEFFREY A. ROSENTHAL
MICHAEL D. DAYAN
CARMINO D. BOCCUZZI, JR.
JEFFREY D. KARP
FRANCISCO L. CESTERO
FRANCESCA L. ODELL
WILLIAM L. MCRAE
JASON FACTOR
JOHN H. KIM
ALAN M. LEVINE
MARGARET S. PEONIS
LISA M. SCHWEITZER
JUAN G. GIRALDEZ
DUANE McLAUGHLIN
CHANTAL E. KORDULA
BENET J. O'REILLY
ADAM E. FLEISHER
SEAN A. O'NEAL
GLENN P. MCGRORY
DEBORAH NORTH
MATTHEW P. SALERNO
MICHAEL J. ALBANO

VICTOR L. HOU
ROGER A. COOPER
LILLIAN TSU
AMY R. SHAPIRO
JENNIFER KENNEDY PARK
ELIZABETH LENAS
LUKE A. BAREFOOT
JONATHAN S. KOLODNER
DANIEL ILAN
MEYER H. FEDIDA
ADRIAN R. LEIPSIC
ELIZABETH VICENS
ADAM J. BRENNEMAN
ARI D. MACKINNON
JAMES E. LANGSTON
JARED GERBER
RISHI ZUTSHI
JANE VANLARE
AUDRY X. CASUSOL
ELIZABETH DYER
DAVID H. HERRINGTON
KIMBERLY R. SPOERRI
JAARON J. MEYERS
DANIEL C. REYNOLDS
ABENA A. MAINOO
HUGH C. CONROY, JR.
JOHN A. KUPIEC
JOSEPH LANZKRON
MAURICER. GINDI
KATHERINE R. REAVES
RAHUL MUKHI
ELANAS S. BRONSON
MANUEL SILVA

KYLE A. HARRIS
LINA BENSMAN
ARON M. ZUCKERMAN
KENNETH S. BLAZEJEWSKI
MARK E. MCDONALD
F. JAMAL FULTON
PAUL V. IMPERATORE
CLAYTON SIMMONS
CHARLES W. ALLEN
JULIA L. PETTY
HELENA K. GRANNIS
SUSANNA E. PARKER
THOMAS S. KESSLER
RESIDENT PARTNERS
JUDITH KASSEL
BOAZ S. MORAG
HEIDE H. ILGENFRITZ
ANDREW WEAVER
CATHERINE S. GRIMM
JOHN V. HARRISON
MATTHEW BRIGHAM
EMILIO MINIVELLE
LAURA BAGARELLA
JONATHAN D.W. GIFFORD
DAVID W.S. YUDIN
KARA A. HAILEY
ANNA KOGAN
BRANDON M. HAMMER
BRIAN J. MORRIS
CARINA S. WALLANCE
ALEXANDER JANGHORBANI
RESIDENT COUNSEL

D: +1 212-225-2912
rmukhi@cgsh.com

November 16, 2023

VIA E-MAIL

Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

Pursuant to Maryland Personal Information Protection Act § 14-3504, we write on behalf of our client, Henry Schein, Inc. and its subsidiaries (together, the “Company” or “Henry Schein”), to notify you of a cybersecurity incident involving approximately two hundred (200) Maryland residents.

IDENTIFICATION OF PARTIES

The entity that experienced the incident is Henry Schein, which is a solutions company for healthcare professionals that provides a number of products and services to dental and medical practitioners and other customers. Henry Schein’s headquarters are located at 135 Duryea Road, Melville, New York 11747.

NATURE OF THE DATA SECURITY INCIDENT

As Henry Schein publicly announced on October 15, 2023, the Company determined on October 14, 2023 that a portion of its manufacturing and distribution businesses experienced a cybersecurity incident. The Company promptly took precautionary action, including taking certain systems offline and other steps intended to contain the incident, which led to the temporary disruption of some of its business operations. Henry Schein also notified relevant law enforcement authorities. In addition, the Company engaged outside cybersecurity and forensic

information technology experts to help investigate any data impact and respond to the situation. The Company's investigation is ongoing.

Henry Schein's ongoing investigation determined that a data breach occurred. The Company maintains personal information on certain of its systems related to its current and former employees, which may have been accessed and obtained by an unauthorized third party as part of the incident. Such information may include, among other things, an individual's name, address, phone number, email address, photograph, date of birth, demographic and background information, government-issued identification numbers (*e.g.*, Social Security number, driver's license or state identification number, passport number), financial information (*e.g.*, bank account information, credit card number, loans), medical history, treatment, and insurance information, details of employment at the Company (*e.g.*, job title, compensation), IP address, and other information. The Company also maintains information for certain dependents of employees that may have been compromised including, among other information, a dependent's name, address, date of birth, demographic information, government-issued identification number (*i.e.*, Social Security number), and other information. The personal information that may have been impacted by the incident depends on, among other things, the particular information that the Company received from employees about themselves and any dependents.

The Company made the decision to notify these potentially affected individuals while its investigation continues.

NUMBER OF INDIVIDUALS

Maryland Residents: Approximately two hundred (200)

Henry Schein is notifying potentially affected individuals in tranches in the interest of providing notice as soon as possible. The number of potentially affected Maryland residents above reflects the number of employees of Henry Schein or its subsidiaries and affiliates who are being notified in the first and second such tranches. The first tranche of notifications will be sent on or about November 17, 2023, and we expect the second tranche will be sent as soon as practical thereafter. Additional tranches may follow. Notice has not been delayed due to a law enforcement investigation. A sample copy of the notice is attached hereto.

STEPS HENRY SCHEIN HAS TAKEN OR PLANS TO TAKE RELATING TO THE INCIDENT

Henry Schein has taken a number of steps to address the incident, and its work remains ongoing. As noted above, upon discovery of the incident, the Company's cybersecurity team immediately took a series of steps, including taking certain systems offline and other steps intended to contain the incident, hiring cybersecurity experts, conducting an investigation to identify and remove any malicious files and determine Company systems that were impacted, and seeking to implement measures to fortify its defenses going forward. The Company also notified and is cooperating with relevant law enforcement authorities.

CREDIT MONITORING

Henry Schein is offering 24 months of identity theft and credit monitoring services to potentially affected Maryland residents free of charge. A sample of the letter to be sent to potentially affected residents offering these services is attached hereto. A description of the services is available here: <https://www.experianidworks.com>.

CONTACT INFORMATION

You may contact me at 212-225-2912 or rmukhi@cgsh.com, or my colleague Jonathan Kolodner at 212-225-2690 or jkolodner@cgsh.com, should you have any questions or need further information.

Respectfully submitted,

A handwritten signature in black ink that reads "Rahul Mukhi". The script is cursive and fluid.

Rahul Mukhi

Attachment



SOLUTIONS FOR HEALTH CARE PROFESSIONALS

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

GENERAL BUSINESS: 631-843-5500

FAX: 631-543-5637

<http://www.henryschein.com>

November 17, 2023

K3551-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01

APT ABC

123 ANY STREET

ANYTOWN, FC 1A2 B3C

COUNTRY



RE: Notice of Data Breach
Please read this entire letter.

To Sample A. Sample:

We write you, as a current employee of Henry Schein, Inc. or one of its subsidiaries (the “Company” or “we”), in connection with the cybersecurity incident the Company previously disclosed and its potential impact on some of your personal information. We take the protection of your information very seriously, and we are contacting you directly to explain the circumstances of the incident and the steps we are taking in response.

What Happened?

As we publicly announced on October 15, 2023, the Company determined on October 14, 2023 that a portion of its manufacturing and distribution businesses experienced a cybersecurity incident. The Company promptly took precautionary action, including taking certain systems offline and other steps intended to contain the incident, which led to the temporary disruption of some of our business operations. We also notified relevant law enforcement authorities.

In addition, the Company engaged outside cybersecurity and forensic information technology experts to help investigate any data impact and respond to the situation. The Company’s investigation is ongoing.

What Information Was Involved?

The Company’s ongoing investigation determined that a data breach occurred. The Company maintains personal information on certain of its systems related to its employees, which may have been accessed and obtained by an unauthorized third party as part of the incident.

The information that the Company maintains for employees may include, among other things, an employee’s name, address, phone number, email address, photograph, date of birth, demographic and background information, government-issued identification numbers (e.g., Social Security number, driver’s license or state identification number, passport number), financial information (e.g., bank account information, credit card number, loans), medical history, treatment, and insurance information, details of employment at the Company (e.g., job title, compensation), IP address, and other information. Further, to the extent provided by an employee, the Company also maintains some of the personal information in the foregoing categories about an employee’s dependents. The Company will be separately notifying and offering credit monitoring to employees’ dependents about whom the Company maintains information.



The personal information that may have been impacted by the incident depends on, among other things, the particular information you have provided to the Company.

What We Are Doing To Protect Your Information

Please be assured that we are doing everything we can to address the incident. Upon discovery of the incident, our cybersecurity team immediately took a series of steps, including taking certain systems offline and other steps intended to contain the incident, hiring cybersecurity experts, conducting an investigation to identify and remove any malicious files and determine company systems that were impacted, and seeking to implement measures to fortify our defenses going forward.

Protecting your personal information is very important to us. To help protect your personal information, we are providing you with identity theft detection and resolution tools through Experian, one of the leading credit and identity monitoring companies, through a complimentary 24-month membership to Experian's® IdentityWorksSM.

To activate this membership and start monitoring your personal information, please follow the steps in Attachment 1.

What You Can Do

We want to make sure you are aware of the additional steps you may take to guard against the unauthorized use of your personal information.

As we all know, cybersecurity incidents increasingly threaten the security of information at work and at home. You should remain vigilant by reviewing account statements and monitoring free credit reports. Please see Attachment 2 for further steps you can take to protect your personal information as well as additional important information. We also encourage you to report any suspicious computer-related activity.

Conclusion

As noted, please see the attachments for instructions on how to enroll in Experian's® IdentityWorksSM, further steps you can take to protect your personal information, and additional important information.

We regret any inconvenience that the incident may cause. Should you have questions or concerns regarding this matter, please call 1-833-603-7299 Monday through Friday, 6 a.m. to 8 p.m. Pacific, and Saturday and Sunday, 8 a.m. to 5 p.m. Pacific (excluding major US holidays).

Sincerely,
Lorelei McGlynn
Senior Vice President, Chief Human Resources Officer

ATTACHMENT 1

How To Enroll In Experian's® IdentityWorksSM

- Ensure that you **enroll by**: February 29, 2024. Your **activation code** will not work after this date.
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: ABCDEFGHI

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-833-603-7299 by February 29, 2024. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

Additional Details Regarding the 24-Month Experian IdentityWorks Membership

A credit card is **not** required for enrollment in Experian IdentityWorks. You may contact Experian **immediately** regarding any fraud issues, and you 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.
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You will receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance¹:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your personal information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-833-603-7299. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent will be 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 Identity Restoration support is available as part of the membership being provided at no cost to you and is effective from the date of this letter. Registration is not required to access the service provided by Experian's Identity Restoration Specialists. 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 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.



ATTACHMENT 2

Monitor Your Accounts

We recommend that you 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 at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, 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
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as a home address or Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
[www.experian.com/
freeze/center.html](http://www.experian.com/freeze/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and 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 you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
[www.experian.com/
fraud/center.html](http://www.experian.com/fraud/center.html)

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
[www.transunion.com/fraud-
victim-resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Monitor Your Personal Health Information

If applicable to your situation, we recommend that you regularly review the explanation of benefits statements that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive the regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the website of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

- Alabama Residents: The Attorney General can be contacted at 1-800-392-5658; or <https://www.alabamaag.gov/consumercomplaint>.
- Alaska Residents: The Attorney General can be contacted at 1031 West 4th Ave., Suite 200, Anchorage, AK 99501-1994; 1-888-576-2529; or http://www.law.alaska.gov/departments/civil/consumer/cp_complaint.html.
- Arizona Residents: The Attorney General can be contacted at 2005 North Central Avenue, Phoenix, AZ 85004; 602-542-5025; or <https://www.azag.gov/consumer/data-breach>.
- Arkansas Residents: The Attorney General can be contacted at 323 Center Street, Suite 200, Little Rock, AR 72201; 1-800-482-8982; consumer@ArkansasAG.gov; or <https://arkansasag.gov/forms/file-a-consumer-complaint/>.
- California Residents: The California Office of Privacy Protection can be contacted at 1300 "I" Street, Sacramento, CA 95814-2919; 800-952-5225; or www.oag.ca.gov/privacy.



- Colorado Residents: The Attorney General can be contacted at 1300 Broadway, 10th Floor, Denver, CO 80203; 720-508-6000; or <https://coag.gov/resources/data-protection-laws/>.
- Connecticut Residents: The Attorney General can be contacted at 165 Capitol Avenue, Hartford, CT 06106; 860-808-5420; or <https://portal.ct.gov/AG/General/Report-a-Breach-of-Security-Involving-Computerized-Data>.
- Delaware Residents: The Delaware Fraud & Consumer Protection Division can be contacted at 820 N. French Street, Wilmington, DE 19801; 302-577- 8600; or <https://attorneygeneral.delaware.gov/fraud/cpu/idtheft/>.
- Florida Residents: The Attorney General can be contacted at 1-866-966-7226; or <https://www.myfloridalegal.com/pages.nsf/Main/18A7753257FE439085256CC9004EC4F7>.
- Georgia Residents: The Attorney General can be contacted at 2 Martin Luther King Jr. Drive, Suite 356, Atlanta, GA 30334-9077; 800-869-1123; or <https://consumer.georgia.gov/consumer-topics/identity-theft-what-do-if-it-happens-you>.
- Hawaii Residents: The Hawaii Department of Commerce and Consumer Affairs can be contacted at 335 Merchant Street, Honolulu, HI 96813; 808-587-3222; or <https://cca.hawaii.gov/identity-theft-information/>.
- Idaho Residents: The Attorney General can be contacted at 700 W. Jefferson Street, P.O. Box 83720, Boise, ID 83720-0010; 208-334-2400; or <https://www.ag.idaho.gov/>.
- Illinois Residents: The Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-800-386-5438; or <https://ccforms submission.ilag.gov/>.
- Indiana Residents: The Attorney General can be contacted at 302 W. Washington Street, 5th Floor, Indianapolis, IN 46204; 1-800-382-5516; or <https://www.in.gov/attorneygeneral/consumer-protection-division/id-theft-prevention/complaint-form>.
- Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319; 515-281-5926; or www.iowaattorneygeneral.gov. You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.
- Kansas Residents: The Attorney General can be contacted at 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597; 785-296-2215; or <https://ag.ks.gov/in-your-corner-kansas/>.
- Kentucky Residents: The Attorney General can be contacted at 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601; (502) 695-5300; or <https://www.ag.ky.gov/Resources/Consumer-Resources/Consumers/Pages/Consumer-Complaints.aspx>.
- Louisiana Residents: The Attorney General can be contacted at 1885 N. Third Street, Baton Rouge, LA 70802; 1-800-351-4889; or <https://www.ag.state.la.us/Page/DataBreach>.
- Maine Residents: The Attorney General can be contacted at 6 State House Station, Augusta, ME 04333; 207-626-8800; or https://www.maine.gov/ag/consumer/complaints/complaint_form.shtml.
- Maryland Residents: The Attorney General can be contacted at 200 St. Paul Place, 25th Floor, Baltimore, MD 21202; 410-576-6491; or <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>. Further information about security breach response and identity theft prevention and protection can be obtained from Maryland's Office of the Attorney General.
- Massachusetts Residents: The Attorney General can be contacted at One Ashburton Place, 18th Floor, Boston, MA 02108; 617-727-8400; or <https://www.mass.gov/how-to/file-a-consumer-complaint#:~:text=You%20can%20reach%20us%20at,time%20using%20our%20online%20form>. You have a right to request from us a copy of any police report filed in connection with 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.
- Michigan Residents: The Attorney General can be contacted at 525 W. Ottawa Street, P.O. Box 30212, Lansing, MI 48909; 877-765-8388; or <https://www.michigan.gov/ag/>.

- Minnesota Residents: The Attorney General can be contacted at 445 Minnesota Street, Suite 1400, St. Paul, MN 55101; (800) 627-3529; or <https://www.ag.state.mn.us/Consumer/Publications/PersonalInformationBreaches.asp>.
- Mississippi Residents: The Attorney General can be contacted at 550 High Street, Jackson MS 39201; 601-359-3680; or <https://www.ago.state.ms.us/divisions/consumer-protection/>.
- Missouri Residents: The Attorney General can be contacted at Supreme Court Building, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102; 800-392-8222; or <https://ago.mo.gov/app/consumercomplaint>.
- Montana Residents: The Attorney General can be contacted at 215 N Sanders Street, Helena, MT 59620-0151; 800-498-6455; or <https://dojmt.gov/consumer/affected-data-breach/>.
- Nebraska Residents: The Attorney General can be contacted at 2115 State Capitol, Lincoln, NE 68509; 800-727-6432; or <https://protectthegoodlife.nebraska.gov/data-breach-notification>.
- Nevada Residents: The Attorney General can be contacted at 100 North Carson Street, Carson City, NV 89701; 702-486-3132; or https://ag.nv.gov/Hot_Topics/Victims/IDTheft/.
- New Hampshire Residents: The Attorney General can be contacted at 33 Capitol Street, Concord, NH 03301; 888-468-4454; or <https://www.doj.nh.gov/consumer/>.
- New Jersey Residents: The Attorney General can be contacted at 124 Halsey Street, Newark, NJ 07101; 973-504-6200; or <https://www.njconsumeraffairs.gov/ocp/Pages/default.aspx>.
- New Mexico Residents: The Attorney General can be contacted at 408 Galisteo Street, Santa Fe, NM 87501; 844-255-9210; or <https://www.nmag.gov/file-a-complaint.aspx>. You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you would get based on information in your credit report; and you may seek damages from a violator. You 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. You can review your 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.
- New York Residents: The Attorney General can be contacted at Office of the Attorney General, The Capitol, Albany, NY 122240341; 1 (800) 771-7755; or <https://ag.ny.gov/internet/privacy-and-identity-theft>. Further information about security breach response and identity theft prevention and protection can be obtained from New York’s Office of the Attorney General.
- North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6000; or <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id-theft/security-breach-information/security-breach-advice/>. Further information about preventing identity theft can be obtained from North Carolina’s Office of the Attorney General.
- North Dakota Residents: The Attorney General can be contacted at 600 E. Boulevard Ave Dept. 125, Bismarck ND 58505; 1-800-472-2600; ndag@nd.gov; or <https://attorneygeneral.nd.gov/consumer-resources/consumer-complaints>.
- Ohio Residents: The Attorney General can be contacted at 30 E. Broad St., 14th Floor Columbus, OH 43215; 800-282-0515; <https://www.ohioattorneygeneral.gov/Files/Forms/Forms-for-Consumers/ConsumerComplaintForm3292012-pdf.aspx>.



- Oklahoma Residents: The Attorney General can be contacted at 313 NE 21st Street, Oklahoma City, OK 73105; 833-681-1895; or <https://www.oag.ok.gov/consumer-protection>.
- Oregon Residents: The Attorney General can be contacted at 877-877-9392; or <https://www.doj.state.or.us/consumer-protection/>. You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.
- Pennsylvania Residents: The Attorney General can be contacted at 16th Floor, Strawberry Square, Harrisburg, PA 17120; 800-441-2555; or <https://www.attorneygeneral.gov/protectyourself/identity-theft/>.
- Puerto Rico Residents: The Puerto Rico Department of Consumer Affairs can be contacted at 787-722-7555; or <https://www.daco.pr.gov/servicios/querellas/>.
- Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, RI 02903; (401) 274-4400; or <https://riag.ri.gov/about-our-office/divisions-and-units/civil-division/public-protection/consumer-protection>. Further information about preventing identity theft can be obtained from the Office of the Attorney General. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You are advised that fees may be required to be paid to the consumer reporting agencies.
- South Carolina Residents: The Attorney General Consumer Affairs Division can be contacted at 293 Greystone Boulevard, Suite 400; 803-734-4200; or <https://consumer.sc.gov/identity-theft-unit>.
- South Dakota Residents: The Attorney General Division of Consumer Protection can be contacted at 1302 E HWY 14, Suite 3, Pierre, SD 57501; 605-773-4400; or <https://consumer.sd.gov/fastfacts/securitybreach.aspx>.
- Tennessee Residents: The Attorney General can be contacted at P.O. Box 20207, Nashville, Tennessee, 37202; (615) 741-4737; or <https://www.tn.gov/content/tn/attorneygeneral/working-for-tennessee/consumer/resources.html>.
- Texas Residents: The Attorney General can be contacted at P.O. Box 12548, Austin, TX, 78711-2548; 800-621-0508; or <https://www.texasattorneygeneral.gov/consumer-protection/identity-theft>. Visit <http://txoag.force.com/CPDOnlineForm> for its consumer complaint form.
- Utah Residents: The Attorney General can be contacted at P.O. Box 142320, Salt Lake City, UT 84114-2320; 801-366-0260; or <https://attorneygeneral.utah.gov/utah-consumer-protection/>.
- Vermont Residents: The Attorney General can be contacted at 109 State St, Montpelier, VT 05609; 800-649-2424; or <https://ago.vermont.gov/privacy-data-security/>.
- Virginia Residents: The Attorney General can be contacted at 804-786-2042; or <https://www.oag.state.va.us/consumer-protection/index.php/get-help/contact-us2>.
- Washington Residents: The Attorney General can be contacted at 800 5th Ave. Ste. 2000, Seattle, WA 98104-3188; 206-464-6684; or more information may be found at <https://www.atg.wa.gov/fileacomplaint.aspx>.
- Washington D.C. Residents: The Attorney General can be contacted at 400 6th Street, NW, Washington, DC 20001; 202-727-3400; or <https://oag.dc.gov/>. Further information about preventing identity theft can be obtained from the Office of the Attorney General.
- West Virginia Residents: The Attorney General can be contacted at State Capitol Complex, Bldg 1, Rm E-26, 1900 Kanawha Blvd E, Charleston, WV 25305; 1-800-368-8808; or <https://ago.wv.gov/consumerprotection/Pages/Identity-Theft-Prevention.aspx>.
- Wisconsin Residents: The Attorney General can be contacted at 2811 Agriculture Dr., P.O. Box 8911, Madison, WI 53708-8911; or (800) 422-7128. For more information on Identity Theft and Privacy Protection, visit: <https://datcp.wi.gov/Pages/Publications/IDTheftPrivacyProtectionFactSheets.aspx>.
- Wyoming Residents: The Attorney General can be contacted at 109 State Capitol, Cheyenne, WY 82002; 1-800-438-5799; or <https://ag.wyo.gov/law-office-division/consumer-protection-and-antitrust-unit>.

CLEARY GOTTlieb STEEN & HAMILTON LLP

AMERICAS
NEW YORK
SAN FRANCISCO
SÃO PAULO
SILICON VALLEY
WASHINGTON, D.C.

ASIA
BEIJING
HONG KONG
SEOUL

One Liberty Plaza
New York, NY 10006-1470
T: +1 212 225 2000
F: +1 212 225 3999
clearygottlieb.com

D: +1 212-225-2912
rmukhi@cgsh.com

EUROPE & MIDDLE EAST
ABU DHABI
BRUSSELS
COLOGNE
FRANKFURT
LONDON
MILAN
PARIS
ROME

October 23, 2024

VIA E-MAIL

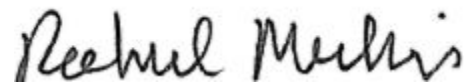
Attorney General Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Dear Attorney General Brown:

I write on behalf of Henry Schein, Inc. (“Henry Schein” or the “Company”) to supplement the Company’s November 16, 2023 notice to your Office regarding a cybersecurity incident that the Company publicly announced on October 15, 2023. Henry Schein’s November 16, 2023 notice to your Office stated that approximately 200 Maryland residents were potentially impacted by the incident. Since the prior notice, the Company continued to investigate the impacted data, including by engaging a third-party expert to perform data mining of the impacted information. The Company’s investigation is now complete and has determined through the data mining process that there were a total of 1,092 Maryland residents whose personal information was impacted.

Henry Schein sent notices to the impacted individuals, which included an offer for two years of complimentary credit monitoring, on a rolling basis during the course of the investigation. The notices were sent to affected Maryland residents on or about November 17, 2023; December 4, 2023; December 29, 2023; January 11, 2024; June 25, 2024; September 5, 2024; and October 16, 2024.

Respectfully submitted,



Rahul Mukhi