



HUNTON ANDREWS KURTH LLP
200 PARK AVENUE
NEW YORK, NY 10166-0005

TEL 212 • 309 • 1000
FAX 212 • 309 • 1100

LISA J. SOTTO
DIRECT DIAL: 212 • 309 • 1223
EMAIL: lsotto@HuntonAK.com

FILE NO: 047791.0000410

August 30, 2023

Via E-Mail (idtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

In accordance with Md. Code Ann., Com. Law § 14-3504, I am writing on behalf of The Estée Lauder Companies Inc. (“ELC” or the “Company”) to notify you regarding the nature and circumstances of a recent data security issue.

On July 11, 2023, ELC learned that an unauthorized third party gained access to some of the Company’s systems. Promptly after learning of the issue, the Company proactively took steps to secure its systems and engaged leading cybersecurity experts to assist with its investigation. ELC also notified and is coordinating with law enforcement regarding this issue.

On August 18, 2023, the Company determined that the unauthorized party obtained, on July 13, 2023, certain personal information of Maryland clinical research panelists. The affected clinical research panelist information varied by individual and included names, contact information, dates of birth, Social Security numbers, demographic information, and certain health-related information (such as allergies). There is approximately one Maryland resident for whom Social Security number was affected by this issue.

On August 10, 2023, the Company determined that the unauthorized party obtained, on July 11, 2023, certain personal information of employees and consultants. The affected employee/consultant information varied by individual and included names, corporate email addresses, work phone numbers, employee ID numbers, work locations, roles (employee or consultant), managers and direct reports, dates of last password change or login, and hashed Company system passwords. On August 22, 2023, ELC determined that, for approximately eight Maryland residents who are employees/consultants of the Company, the unauthorized party was able to determine clear-text Company system passwords.

August 30, 2023
Office of the Attorney General
Page 2

ELC has implemented additional monitoring and security measures to help further protect its systems. These measures include proactively disabling affected systems in an effort to contain the incident and implementing measures to reset employee passwords.

Attached for reference are copies of the notices the Company is sending to the affected Maryland residents. Please do not hesitate to contact me if you have any questions.

Very truly yours,



Lisa J. Sotto

Enclosure

NOTICE OF DATA BREACH

We recently learned of a data security incident affecting our company.

What Happened?

On August 18, 2023, we determined through our ongoing investigation that an unauthorized third party gained access to some of our systems and, on or around July 13, 2023, obtained personal information of certain Clinical Research Center panelists, including you.

What Information Was Involved?

The personal information obtained includes name, contact information, date of birth, Social Security number, demographic information, and certain health-related information that you have provided (such as allergies). The impacted data varies for each affected individual.

What We Are Doing

After learning of the incident, we quickly launched an investigation and have been working with leading outside cybersecurity experts to determine the nature and scope of the issue. We are also coordinating with law enforcement authorities. We take the security of our data and systems very seriously and have put in place additional monitoring measures to further protect our systems.

What You Can Do

We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your free credit reports. If you'd like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. The contact information is below. We also recommend that you remain alert for unsolicited communications involving your personal information.

In addition, we have arranged to offer identity protection and credit monitoring services to affected panelists for two years at no cost to them. The attached Reference Guide provides information on registration and recommendations by the U.S. Federal Trade Commission on the protection of personal information.

For More Information

We regret any inconvenience this incident may have caused you. If you have any questions regarding this incident, please contact us at [insert telephone number] [insert days and times of operation].

Reference Guide

We encourage affected Clinical Research Center panelists to take the following steps:

Register for Identity Protection and Credit Monitoring Services. We have arranged with [Insert Name] to help you protect your identity and your credit information for two years at no cost to you. [Insert details of services]

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
 Consumer Response Center
 600 Pennsylvania Avenue, NW
 Washington, DC 20580
 1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)

- Proof of your current residential address (such as a current utility bill or account statement)

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/internet/resource-center>

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft. You can contact the North Carolina Attorney General at:

North Carolina Attorney General's Office
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226 (toll-free in North Carolina)
(919) 716-6400
www.ncdoj.gov

Important Information About Cybersecurity Incident

As a follow-up to the July 2023 email sent to employees, we are writing to provide an update on the recent cybersecurity incident with further information and suggestions for you.

What Happened

As we previously communicated in July, an unauthorized third party gained access to some of our Company's systems. Through our ongoing investigation, ELC determined that an unauthorized third party obtained ELC's Company directory data on or around July 11, 2023.

What Information Was Involved

The Company directory data **does not include** banking information, Social Security or national identification numbers, compensation details, or health information.

The affected information includes employee and consultant name, corporate email address, work phone numbers, employee ID number, work location, role (employee or consultant), manager and direct reports, and date of last password change or login. In addition, Company system passwords belonging to employees and consultants were also obtained.

What We Are Doing

As we communicated in July, after learning of the incident, we quickly launched an investigation and have been working with leading outside cybersecurity experts to determine the cause, nature, and scope of the issue. We are also coordinating with law enforcement authorities. We take the security of our data and systems very seriously and have put in place additional monitoring measures to further protect our systems.

Where available, we are currently offering optional identity monitoring services at no cost to you. Please follow the [link](#) to learn how to sign up for these services.

What You Can Do

If you have not already done so within the past month, please change your Company system password as soon as possible. Sign into ELC VPN, go to passport.elcompanies.com to change your password, and follow the [link](#) for further guidance. In addition, we recommend you change your password for any other online account on which you used a password that is the same or similar to your Company system password. Because the incident involved your email address, we also recommend that you remain alert for any unsolicited communications involving your personal information to help protect against phishing. As a reminder, for full details on how to report suspicious activity, please see this guide: [How to Report Suspicious Messages](#).

As mentioned above, where available, we are currently offering optional identity monitoring services at no cost to you. Please follow the [link](#) to learn how to sign up for these services.

For More Information:

If you have any questions regarding this issue, please call OneSource at 1-844-472-8352 (1-844-HR at ELC) in the U.S. or Canada from 8a.m.–8 p.m. EST or [click here](#) for your local OneSource number. You may also refer to the [MyELC Frequently Asked Questions](#) page or contact your HR business partner. You may receive additional updates regarding this incident, as appropriate.

Thank you very much for your cooperation and understanding.

Additional Disclosures for U.S. Residents

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's ("FTC's") website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three nationwide consumer reporting agencies provide free annual credit reports only through the website, toll-free number or request form.

When you receive your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you haven't requested credit. Some companies bill under names other than their store or commercial names. The consumer reporting agency will be able to tell you when that is the case. Look in the "personal information" section for any inaccuracies in your information (such as your home address and Social Security number). If you see anything you do not understand, call the consumer reporting agency at the telephone number on the report. Errors in this information may be a warning sign of possible identity theft. You should notify the consumer reporting agencies of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate consumer reporting agency by telephone and in writing. Consumer reporting agency staff will review your report with you. If the information cannot be explained, then you will need to call the creditors involved. Information that cannot be explained also should be reported to your local police or sheriff's office because it may signal criminal activity.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For streamlined checklists and sample letters to help guide you through the recovery process, please visit <https://www.identitytheft.gov/>
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others who may require proof of the identity theft crime.

You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft and how to repair identity theft:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580

1-877-IDTHEFT (438-4338)

www.ftc.gov/idtheft/

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be the victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can place a fraud alert on your credit report by calling any one of the toll-free numbers provided below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three consumer reporting agencies. For more information on fraud alerts, you also may contact the FTC as described above.

Equifax	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	www.equifax.com
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	www.experian.com
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19016	1-800-680-7289	www.transunion.com

Consider Placing a Security Freeze on Your Credit File. You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually. There is no charge to place or lift a security freeze. For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above. As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information.

The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (such as a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports.

For Maryland Residents. You can obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft. You may contact the Maryland Attorney General at:

Maryland Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023 (toll-free in Maryland)
(410) 576-6300
www.oag.state.md.us

For New York Residents. You can obtain information from the New York State Office of the Attorney General about how to protect yourself from identity theft and tips on how to protect your privacy online. You can contact the New York State Office of the Attorney General at:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
1-800-771-7755 (toll-free)
1-800-788-9898 (TDD/TTY toll-free line)
<https://ag.ny.gov/>

Bureau of Internet and Technology (BIT)
28 Liberty Street
New York, NY 10005
Phone: (212) 416-8433
<https://ag.ny.gov/internet/resource-center>

For Oregon Residents. We encourage you to report suspected identity theft to the Oregon Attorney General at:

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301-4096
(877) 877-9392 (toll-free in Oregon)
(503) 378-4400
<http://www.doj.state.or.us>

For Washington, D.C. Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
441 4th Street NW
Suite 1100 South
Washington, D.C. 20001
(202)-727-3400
<https://oag.dc.gov/>

#