



Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

March 22, 2021

By Electronic Mail

Office of the New Hampshire Attorney General
Consumer Protection Bureau
Attn: Security Breach Notification
DOJ-CPB@doj.nh.gov

To Whom It May Concern:

I am writing on behalf of Underwriters Laboratories Inc., UL Inc., and their subsidiaries and affiliated companies (collectively "UL" or "Company") to inform you of an incident that may have impacted personal information of two (2) New Hampshire residents collected in association with the residents' employment with a UL entity. UL is a global certification company that provides services to businesses and other organizations. UL is headquartered at 333 Pfingsten Road, Northbrook, IL, 60062.

On February 13, 2021, UL detected unusual activity on its systems. UL promptly shut down systems as a precaution and engaged leading cybersecurity experts to assist with an investigation to determine the nature and scope of the incident. UL also notified law enforcement. By February 21, 2021, UL determined that the incident resulted in unauthorized access to certain personal information. UL then began to identify whose personal information was accessed and worked to assemble and verify available contact information. UL is not aware of any evidence indicating that personal information affected by this incident has been sold or is being misused. UL's investigation into the scope of the incident and the personal information potentially affected is ongoing.

To date, UL has concluded that the incident impacted names, dates of birth, and Social Security numbers. The Company has taken multiple steps to reduce the risks of this type of incident recurring, including resetting user credentials to access Company systems and deploying additional monitoring tools.

UL will send notice by email to the impacted New Hampshire residents on March 23, 2021. We enclose a sample notice in this notification. In addition to providing information regarding credit reporting agencies, security freezes, fraud alerts, and other identity theft prevention tools, the Company is offering credit monitoring and identity protection services for 2 years through Experian, at no cost to the impacted residents.

[Continued on next page]

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

A handwritten signature in black ink, appearing to read "W. James Denvil". The signature is written in a cursive style with a large initial "W" and a prominent flourish at the end.

James Denvil

Counsel
w.james.denvil@hoganlovells.com
D +1 (202) 637-5521

Enclosure



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

We are writing to let you know that Underwriters Laboratories Inc., UL Inc., and their subsidiaries and affiliated companies experienced a cybersecurity incident that impacted personal information related to you.

WHAT HAPPENED

On February 13, 2021, UL detected unusual activity on its systems. UL promptly shut down systems as a precaution and engaged leading cybersecurity experts to assist with an investigation to determine the nature and scope of the incident. UL notified law enforcement. By February 21, 2021, UL determined that the incident resulted in unauthorized access to certain personal information. UL then began to identify whose personal information was accessed and worked to assemble and verify available contact information. Although we are not aware of any evidence indicating that your personal information has been sold or is being misused, we are providing this notice out of an abundance of caution so that you can take steps to protect yourself.

WHAT INFORMATION WAS INVOLVED

The incident impacted your name, Social Security number, and date of birth.

WHAT WE ARE DOING

The trust our employees place in UL is our top priority. We have taken multiple steps to reduce the risks of this type of an incident happening, for example we have reset user credentials to access our systems and deployed additional monitoring tools. Additionally, we have arranged for you to obtain credit monitoring and identity theft protection services at no cost to you for two years through Experian, a leading provider of credit monitoring and identity protection services. Information regarding the package of services is included in Attachment 2 to this letter.

WHAT YOU CAN DO

We are not aware of any evidence indicating that your personal information has been sold or is being misused. Out of an abundance of caution, we recommend that you remain vigilant and review your financial records and statements for signs of suspicious activity. Please find additional information in Attachment 1 to this letter. As noted above, you can enroll, at no cost to you, in the Experian credit monitoring and identity theft prevention services. Information about enrollment is contained in Attachment 2 to this letter.

FOR MORE INFORMATION

If you have any questions or need additional information, please call 1-???-???-????, Monday through Friday from 8:00 am to 5:30 pm Central Time.

We apologize for any inconvenience this may cause.

Sincerely,

Linda Chapin
EVP & Chief Human Resources Officer | UL Inc.
333 Pfingsten Road | Northbrook, IL 60062

Enclosures

Attachment 1: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at <https://www.consumer.ftc.gov/articles/0003-phishing>.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. If you are a resident of Rhode Island, you have the right to obtain a police report. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Whether or not you enroll in the credit monitoring product offered, we recommend that you consider placing a free "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Fraud alerts last one year. Identity theft victims can get an extended fraud alert for seven years.

Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting companies is:

Equifax PO Box 740256 Atlanta, GA 30374 www.equifax.com/personal/credit-report-services/credit-fraud-alerts/ 1-800-525-6285	TransUnion PO Box 2000 Chester, PA 19016 www.transunion.com/fraud 1-800-680-7289	Experian PO Box 9554 Allen, TX 75013 www.experian.com/fraud 1-888-397-3742
---	--	--

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself. If you are a resident of the District of Columbia, Maryland, North Carolina, Iowa, Oregon, or Rhode Island, you can also reach out to your respective state's Attorney General's office at the contact information below. All other residents can find information on how to contact your state attorney general at <https://www.naag.org/find-my-ag/>.

Federal Trade Commission

Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357) / www.ftc.gov/idtheft

North Carolina Attorney General's Office

90001 Mail Service Center
Raleigh, NC 27699
1-919-716-6400 / <https://ncdoj.gov/>

Oregon Department of Justice

1162 Court Street NE
Salem, OR 97301
1-877-877-9392 / <https://justice.oregon.gov>

Office of the Attorney General for the District of Columbia

400 6th Street NW
Washington, D.C. 20001
1-202-727-3400 / oag.dc.gov

Maryland Attorney General's Office

200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 / www.marylandattorneygeneral.gov

Rhode Island Attorney General's Office

150 South Main Street
Providence, Rhode Island 02903
1-401-274-4400 / <http://www.riag.ri.gov>

Consumer Protection Division**Office of the Attorney General of Iowa**

1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926 / www.iowaattorneygeneral.gov

Security Freeze Information

You have the right to request a free Security Freeze (aka "Credit Freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a Credit Freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A Credit Freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax Security Freeze

PO Box 105788
Atlanta, GA 30348
<http://www.equifax.com/personal/credit-report-services/credit-freeze/>
1-800-349-9960

TransUnion Security Freeze

PO Box 2000
Chester, PA 19016
www.transunion.com/freeze
1-888-909-8872

Experian Security Freeze

PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

To request a Credit Freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)

Attachment 2: Credit Monitoring and Identity Theft Services Enrollment Information

To help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: <<b2b_text_1(EnrollmentDeadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bplus>
- Provide your **activation code**: <<Member ID>>

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 877.288.8057 by <<b2b_text_1(EnrollmentDeadline)>> Be prepared to provide engagement number <<b2b_text_2(EngagementNumber)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & 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 Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was 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 877.288.8057. 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 one year 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.

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

** 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.