



20 Church Street  
20th Floor  
Hartford, CT 06103  
Telephone: 860-525-5065  
Fax: 860-527-4198  
www.lockelord.com

Theodore P. Augustinos

August 10, 2021

Office of the Attorney General  
Consumer Protection Bureau  
33 Capitol Street  
Concord, NH 03301  
DOJ-CFB@doj.nh.gov

Re: Lydall, Inc.  
Supplement to Notice dated April 23, 2021 pursuant to N.H. Rev. Stat. § 359-C:19

Dear Attorney General Formella:

On behalf of our client Lydall, Inc., we hereby supplement the notice dated April 23, 2021 pursuant to N.H. Rev. Stat. § 359-C:19 of a security incident involving potential disclosure of the personal information of approximately 145 New Hampshire residents. Based on Lydall's continued investigation into this incident, Lydall has determined that the incident affected additional individuals, including 119 New Hampshire residents. Therefore, the personal information of a total of 264 New Hampshire residents was affected by this incident. At this stage, Lydall's investigation into the incident is complete and Lydall does not expect additional affected individuals subsequent to this disclosure.

#### *What Happened*

The facts of the incident were provided by the initial notice dated April 23, 2021. As indicated in the initial notice, the investigation into this incident was ongoing at that time. Upon completion of the investigation, including exhaustive review of the data exposed in the incident, Lydall identified that the personal information of additional individuals had been exposed. These additional individuals are former employees of Lydall and their dependents. Due to the nature and format of the potentially compromised information, Lydall expended significant internal and external resources in an exhaustive data mining effort to identify affected individuals. This effort identified a group of individuals who were notified in April 2021, and ultimately identified additional individuals, most of whom were notified on or about July 28, 2021, and the remainder of whom were notified on or about August 9, 2021.

To date, there is no indication that the information compromised in the ransomware attack has been published, further disclosed, or misused.

August 10, 2021  
Page 2

*What Information Was Involved*

Based on Lydall's investigation, which is now complete, it appears that the personal information exposed in this incident included the types of information described in our initial notice: affected individuals' names, addresses, personal email addresses and telephone numbers, dates of birth, social security numbers, certain health and medical information, health insurance information, ethnicity (to the extent provided to Lydall by the affected individual), and direct deposit information (including financial account number).

*What Lydall is Doing*

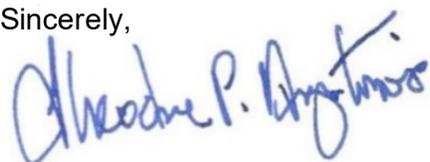
As described in the initial notice, immediately upon the discovery of the attack, Lydall took steps to terminate it and prevent any further unauthorized access. As required by N.H. Rev. Stat. § 359-C:20(I), Lydall provided notice of this incident by mail on or about April 26, 2021 to the affected individuals known at that time. A template for that notification letter was provided as an enclosure to our initial notice to your office. Having identified additional affected individuals, Lydall notified them of the incident by mail on July 28, 2021 and on August 9, 2021. A template for the notification letter to these additional individuals is enclosed. The notification letter describes Lydall's offer of credit monitoring services for two years at no cost to the affected individuals, and provides additional guidance for affected individuals to protect themselves. Lydall is also reviewing and enhancing its safeguards to mitigate the risk of further or future compromises of personal information.

On behalf of Lydall, we are notifying state agencies as required in jurisdictions where additional affected individuals reside.

\* \* \* \* \*

Please do not hesitate to contact me with any questions related to this matter.

Sincerely,



Theodore P. Augustinos

Enclosure



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Re: Important Notice Regarding Potential Disclosure of Your Personal Information

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>:

Lydall, Inc. is contacting you about a security incident involving potential disclosure of your personal information. As described below, we experienced a ransomware attack that resulted in the potential acquisition of your personal information that were contained in our Human Resources files as a spouse or dependent of one of our employees or former employees. As a result, Lydall is notifying you of this incident and providing you with tools to help you protect yourself against potential identify theft. If other members of your household or other dependents were affected by this incident, they will receive separate letters.

#### **What Happened**

On March 24, 2021 Lydall discovered an attempted ransomware attack on certain of our systems. Lydall immediately terminated the attack and began to investigate, and engaged an outside law firm and outside forensics investigators to determine the scope and nature of the attack, and the extent to which the security of personal and corporate information may have been compromised. <<b2b\_text\_3(RIStatement)>>

Based on the forensic investigation, Lydall learned that the compromised information included personal information of our employees and former employees. The investigation recently determined that the compromised information also included certain information of their spouses and dependents. To date, the forensic investigation could not conclude definitely whether the information was actually acquired by the attacker, and we have found no indication that any of the compromised information has been misused, or published or otherwise disclosed. Nevertheless, we are notifying you so that you can take steps to protect your identity, as further described below.

#### **What Information Was Involved**

Your personal information that was potentially exposed to unauthorized access or acquisition may have included your name, address, personal email address and telephone number, date of birth, Social Security number, certain health and medical information, health insurance information, ethnicity (to the extent you provided it to Lydall), and direct deposit information (including financial account number). We have no indication that your personal information has been misused, but we wanted to make you aware of the incident, our efforts to safeguard your personal information, and resources you may use to protect yourself.

#### **What We Are Doing**

We took immediate steps upon the discovery of the attack to terminate the attack and prevent any further unauthorized access to personal information. We have attached instructions to this letter for credit monitoring services we are offering at no cost to you for two years, and information on further steps you can take to protect yourself against identity theft and fraud. We have also been in contact with legal counsel, and law enforcement and regulatory authorities.

**What You Can Do**

As always, we recommend that you remain vigilant and review your account statements and credit reports regularly, and report any concerning transactions to your financial services provider. To assist you in protecting yourself against risks related to this incident, we are offering complimentary access to Experian IdentityWorks<sup>SM</sup> for two years. Enclosed with this letter is information regarding these services and instructions for enrollment, as well as additional information regarding steps you can take to protect yourself against identity theft and fraud. If you have questions, please call 1-800-851-1111, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Time, excluding some U.S. holidays.

We sincerely apologize for any inconvenience or concern this situation may cause. Again, we want to reassure you that we have taken steps to improve the security of personal information entrusted to us.

Sincerely,



Randall Gonzales  
Executive Vice President & Chief Financial Officer

To help protect your identity, we are offering a **complimentary** two-year membership of Experian IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b\_text\_1(EnrollmentDeadline)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: <https://www.experianidworks.com/3bcredit>
3. PROVIDE the **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. 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 TWO YEAR EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at <https://www.experianidworks.com/3bcredit> or call 877-288-8057 to register with the activation code above.**

**What you can do to protect your information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

\* 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.

## Additional Information and U.S. State Notification Requirements

There are a number of steps you should consider to guard against identity theft.

**Review Your Account Statements and Credit Report:** It is recommended that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. Report any fraudulent transactions to the creditor or credit reporting agency from whom you received the statement or report. You may obtain a free copy of your credit report from each credit reporting agency once every 12 months, whether or not you suspect any unauthorized activity on your account, by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form available at that website and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report at any time by contacting any one or more of the national credit reporting agencies listed below.

### **Equifax**

P.O. Box 740241  
Atlanta, Georgia 30374  
[www.equifax.com](http://www.equifax.com)  
1-800-685-1111 Credit Reports  
1-888-766-0008 Fraud Alert  
1-800-685-1111 Security Freeze

### **Experian**

P.O. Box 2002  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
1-888-397-3742 Credit Reports  
1-888-397-3742 Fraud Alert  
1-888-397-3742 Security Freeze

### **TransUnion (FVAD)**

P.O. Box 105281  
Atlanta, GA 30348-5281  
[www.transunion.com](http://www.transunion.com)  
1-800-888-4213 Credit Reports  
1-800-680-7289 Fraud Alert  
1-800-680-7289 Security Freeze

**Federal Trade Commission (FTC) and State Resources:** General guidance on protecting yourself from identify theft is available from the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington D.C. 20580, by phone at 877-ID-THEFT (438-4338), and/or from the FTC website at <http://www.ftc.gov/bcp/edu/microsites/idtheft>. In many states, additional information is also available from your state's Attorney General's Office.

**Fraud Alerts and Security Freezes:** You may obtain information about fraud alerts and security freezes (also referred to as credit freezes), including how to place a fraud alert or security freeze, from the Federal Trade Commission or credit reporting agencies at the contact information provided above. However, be aware that a fraud alert or security freeze, may interfere with or delay legitimate requests for credit approval. You'll need to supply your name, address, date of birth, Social Security number and other personal information in order to place a security freeze on your credit.

### For residents of Massachusetts:

State law advises you that you have the right to obtain a police report. You also will not be charged for seeking a security freeze, as described above in this document.

### For residents of Rhode Island:

To contact the Rhode Island Attorney General; (401) 274-4400 or check <http://www.riag.ri.gov/home/ContactUs.php>

### For residents of Iowa:

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

### For residents of Oregon:

State law advises you to report any suspected identity theft to law enforcement, as well as the FTC.

### For residents of Maryland and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General about steps you can take to avoid identity theft.

### **Maryland Office of the Attorney General**

Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

### **North Carolina Office of the Attorney General**

Consumer Protection Division  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-566-7226  
[www.ncdoj.com](http://www.ncdoj.com)