

India Vincent
ivincen@burr.com
Direct Dial: (205) 458-5284
Direct Fax: (205) 244-5714

Burr & Forman LLP
420 North 20th Street
Suite 3400
Birmingham, AL 35203

Office (205) 251-3000
Fax (205) 458-5100

BURR.COM

December 4, 2020

VIA FEDEX

Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

RECEIVED

DEC 08 2020

CONSUMER PROTECTION

**Re: Database Breach Notification under New Hampshire Revised Statutes,
Title XXXI, § 359-C:20**

Attorney General Gordon J. MacDonald:

We are providing this notice to you in accordance with New Hampshire Revised Statutes, Title XXXI, § 359-C:20 on behalf of our firm's client, Dunn Investment Company and its subsidiaries (collectively, the "Company").

Synopsis of the Events Surrounding the Breach:

On September 30th, 2020, some of Company's computer systems were attacked by ransomware. The Company became aware of the attack that morning and took steps to contain the intrusion. However, some computers were infected. In response to this attack, the Company restored server data from recent backups, and remediated impacted PCs.

The Company's investigation revealed that the infected computers included a server that contained personnel, payroll and supplier information. This information included names and addresses of active and inactive employees along with their Social Security numbers, dates of birth and employee ID numbers (the "Personnel Database"). In some cases, the Personnel Database contained bank account numbers (used for direct deposit) and driver's license numbers. At this point, the Company does not know that any of this personal information was extracted by the criminal actor.

What Has the Company Done

The Company has already implemented additional technology recommended by one of its technical consultants to help defend against future attacks. Additionally, the Company is continuing to review the incident and recommendations from technical consultants to determine if any further remedial actions are appropriate.

Impact on New Hampshire Resident

According to the Company's records, there is one (1) New Hampshire resident whose personal information was stored in the Personnel Database. Attached hereto as Exhibit A is a copy of the form of notice that the Company is providing to the New Hampshire resident this week.

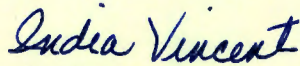
Attorney General Gordon J. MacDonald
December 4, 2020
Page 2

Services Offered by the Company

Although the Company believes the risk of harm from this incident is limited, out of an abundance of caution, the Company is offering these New Hampshire residents, one year of Norton LifeLock's Defender identity protection services, free of charge.

If you require any further information about the incident, please let me know.

Very truly yours,



India Vincent

IEV/
Attachment

Exhibit A
Notice To New Hampshire Resident

See attached

BURR FORMAN



December 4, 2020

[RETURN ADDRESS]
[CITY, STATE ZIP]

[Name]
[Address1]
[Address2]
[City, State Zip]

NOTICE OF SECURITY INCIDENT

As a valued employee or supplier, we wanted you to be aware of an issue that may involve your personal information. We understand the importance of your privacy and ask that you please review this letter.

WHAT HAPPENED?

On September 30th, 2020, some of the Company's computer systems were attacked by ransomware. We became aware of the attack that morning and took steps to contain the intrusion. However, some computers were infected. In response to this attack, we restored server data from recent back-ups, and remediated impacted PCs.

WHAT INFORMATION WAS INVOLVED?

Our investigation of the incident revealed that the infected computers included a server that contained personnel, payroll and supplier information. This included names and addresses of active and inactive employees along with their Social Security numbers. In some cases, the database contained bank account numbers (used for direct deposit) and driver's license numbers. Supplier information was also stored on that server, and that included Social Security numbers for suppliers who use their Social Security numbers for their business. However, at this point, have no indication that this information was extracted by the criminal actor.

WHAT WE ARE DOING

We regret this event occurred. This notice is provided so you can be aware of the incident and have an opportunity to take additional steps to monitor your credit and financial accounts. In addition, to help ensure you are protected, we are providing to all employees, inactive employees who were in the database, and suppliers whose Social Security numbers were in the database one year of complimentary **LifeLock Defender™** identity theft protection service. Instructions for activating your complimentary service are on the back of this letter.

We have already implemented additional technology recommended by one of our technical consultants to help defend against future attacks. We plan to supplement existing security to help us further protect information of our employees and suppliers in the future.

WHAT YOU CAN DO

Please review the attachment to this letter, "Steps You Can Take to Further Protect Your Information". Among other things, this attachment provides the contact information for three major credit reporting agencies.

FOR MORE INFORMATION

For further information and assistance, please contact the Company's dedicated Norton LifeLock Help Line at [INSERT 800 NUMBER]. The help line is available twenty-four hours a day, seven days a week until March 15, 2021.

We apologize for this inconvenience. Thank you.

Sincerely,

EXAMPLE

Chief Financial Officer

To activate your complimentary LifeLock Defender™ membership:

1. In your web browser, go directly to **www.LifeLock.com**. Click on the yellow “**START MEMBERSHIP**” button (*do not attempt registration from a link presented by a search engine*).
2. You will be taken to another page where, **below the FOUR protection plan boxes**, you may enter the **Promo Code: <<PROMO CODE>>** and click the “**APPLY**” button.
3. On the next screen, enter your **Member ID: <<MEMBER ID>>** and click the “**APPLY**” button.
4. Your complimentary offer is presented. Click the red “**START YOUR MEMBERSHIP**” button.
5. Once enrollment is completed, you will receive a confirmation email (*be sure to follow ALL directions in this email*).

**Alternatively, to activate your membership over the phone,
please call: <<ENROLLMENT PHONE #>>**

You will have until March 15, 2021 to enroll in this service.

Once you have completed the LifeLock enrollment process, the service will be in effect. Your **LifeLock Defender™** membership includes:

- ✓ Primary Identity Alert System¹
- ✓ 24/7 Live Member Support
- ✓ Dark Web Monitoring²
- ✓ Norton™ Security Deluxe³ (90 Day Free Subscription)
- ✓ Stolen Funds Reimbursement up to \$25,000⁴
- ✓ Personal Expense Compensation up to \$25,000⁴
- ✓ Coverage for Lawyers and Experts up to \$1 million⁴
- ✓ U.S.-based Identity Restoration Team

No one can prevent all identity theft or cybercrime.

¹ LifeLock does not monitor all transactions at all businesses.

² These features are not enabled upon enrollment. Member must take action to get their protection.

³ Norton Security Online provides protection against viruses, spyware, malware, and other online threats for up to 5 PCs, Macs, Android devices. Norton account features not supported in this edition of Norton Security Online. As a result, some mobile features for Android are not available such as anti-theft and mobile contacts backup. iOS is not supported.

⁴ Reimbursement and Expense Compensation, each with limits of up to \$25,000 for Defender. And up to \$1 million for coverage for lawyers and experts if needed. Benefits under the Master Policy are issued and covered by United Specialty Insurance Company (State National Insurance Company, Inc. for NY State members). Policy terms, conditions and exclusions at: LifeLock.com/legal.

Steps You Can Take to Further Protect Your Information

- **Review Your Account Statements and Notify Law Enforcement of Suspicious Activity**

As a precautionary measure, we encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits, and monitoring your free credit reports for suspicious activity and errors. If you detect any suspicious activity on an account, promptly notify the financial institution or company with which the account is maintained. You should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your local law enforcement, state attorney general, and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov, call 877-ID-THEFT (877-438-4338), or mail your complaint to the FTC at 600 Pennsylvania Avenue, NW, Washington, DC 20580, using OMB CONTROL#: 3084-0169. Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. You can access these reports at <http://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can find the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Alternatively, you can purchase a copy of your credit report by contacting one of the three national credit reporting agencies, and their contact information is provided here:

Equifax
866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
888-397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
800-888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

You might consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>. You can also obtain information from the FTC and consumer reporting agencies about fraud alerts.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>.

For more information, visit IdentityTheft.gov, call 877-ID-THEFT (877-438-4338), or mail the FTC at 600 Pennsylvania Avenue, NW, Washington, DC 20580, using OMB CONTROL#: 3084-0169. A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

Maryland residents may review information provided by the Maryland Attorney General on avoiding identity theft at <http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by emailing idtheft@oag.state.md.us, writing to 200 St. Paul Place, Baltimore, MD 21202, or calling 410-576-6491.

New York residents may review information about the incident response and identity theft prevention and protection provided by the New York Attorney General at <https://ag.ny.gov/consumer-frauds-bureau/identity-theft> or by calling 800-771-7755.

North Carolina residents may review information provided by the North Carolina Attorney General about preventing identity theft at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>, by calling 877-566-7226, or by writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.

OTHER IMPORTANT INFORMATION

- **Security Freeze**

In some US states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the credit reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze. You may obtain more information about security freezes from the FTC and consumer reporting agencies.