



Robert L. Slaughter III
633 West 5th Street, Suite 4000
Los Angeles, California 90071
Robert.Slaughter@lewisbrisbois.com
Direct: 213.680.5028

May 29, 2020

File No. 34181.496

VIA EMAIL

Attorney General Gordon MacDonald
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
Email: Doj.cpb@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent David S. Lapine Co., Inc. ("Lapine"), a merchandising solutions company headquartered in Stamford, Connecticut. This letter is sent on behalf of Lapine because personal information belonging to a New Hampshire resident may have been affected by a recent data security incident. This information may have included unauthorized access to the individual's name and Social Security number.

On April 9, 2020, Lapine became aware of unusual activity within its network environment and discovered that it had been the victim of data encryption by an unknown third party in an effort to extort money from Lapine. Upon discovering this activity, Lapine took immediate steps to secure its network environment and launched an internal investigation. In the course of this investigation, Lapine engaged a leading independent computer forensics firm to determine what happened and whether any information was affected as a result. On April 22, 2020, Lapine's investigation determined that several files were downloaded by the third party. As a result, Lapine undertook to review the files to determine what information was contained therein. On May 4, 2020, our investigation revealed that some individuals' personal information may have been contained within the affected data. Since that time, we have been working diligently to identify contact information for the individuals potentially affected by this incident. On May 14, 2020, Lapine identified one (1) New Hampshire resident within the potentially affected population.

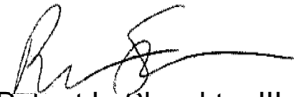
Lapine will be notifying the potentially affected New Hampshire resident on June 1, 2020, via the attached consumer notification template. Lapine is offering twenty-four (24) months of complimentary credit monitoring and identity protection services to the potentially affected resident.

Attorney General Gordon MacDonald
May 29, 2020
Page 2

At this time, Lapine is not aware of any fraudulent activity resulting from this incident. Additionally, Lapine has taken measures to further increase the security of its network environment in the wake of this incident to minimize the possibility of a similar incident occurring in the future.

Please contact me should you have any questions.

Very truly yours,

A handwritten signature in black ink, appearing to read 'R. Slaughter III', with a long horizontal flourish extending to the right.

Robert L. Slaughter III of
LEWIS BRISBOIS BISGAARD & SMITH LLP

RLS:ALW

Attachment: New Hampshire Notification Letter Template

4836-2317-3820.1



LAPINE

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR, 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.myidcare.com/account-creation/protect>
Enrollment Code:
<<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

June 1, 2020

Re: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a data security incident that may have involved your personal information. At David S. Lapine Co., Inc. (“Lapine”), we take the privacy and security of personal information very seriously and as such I am notifying you of the incident, offering you credit monitoring and identity protection services, and providing you with information about steps you can take to help protect your personal information.

What Happened? On April 9, 2020, Lapine became aware of unusual activity within its network environment and discovered that it had been the victim of data encryption by an unknown third party in an effort to extort money from Lapine. Upon discovering this activity, we took immediate steps to secure our network environment and launched an internal investigation. In the course of this investigation, we engaged a leading independent computer forensics firm to determine what happened and whether any information was affected as a result. On April 22, 2020, our investigation determined that several Lapine files were downloaded by the third party. As a result, we undertook to review the files to determine what information was contained therein. On May 4, 2020, our investigation revealed that some of your personal information may have been contained within the affected data. Since that time, we have been working diligently to identify contact information for the individuals potentially affected by this incident.

At this time, we have no evidence to indicate that the information involved in this incident has been misused. Nonetheless, Lapine takes the security and privacy of personal information very seriously, which is why we are writing to inform you of the incident and to provide you with access to credit monitoring and identity protection services at no cost.

What Information Was Involved? The potentially affected information included your <<variabletext>>.

What We Are Doing? As soon as we discovered the incident, we took the steps described above. We have also taken measures to further increase the security of our network environment in order to minimize the likelihood of a similar event occurring in the future.

As an added precaution, we are offering complimentary identity theft protection services through ID Experts®, a data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.



What You Can Do: You can follow the recommendations included with this letter to protect your personal information. We strongly encourage that you enroll in the complimentary credit monitoring and identity monitoring services we are offering through ID Experts to further protect your personal information. To enroll, please visit <https://app.myidcare.com/account-creation/protect> or call 1-800-939-4170 and use the Enrollment Code provided above. Please note the deadline to enroll in these services is September 1, 2020. To activate credit monitoring you must be over the age of 18, and have established credit in the U.S., a Social Security number in your name, and a U.S. residential address associated with your credit file.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions, please contact our team at <https://app.myidcare.com/account-creation/protect> between 9:00 am and 9:00 pm Eastern time. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Noah Lapine', with a stylized flourish at the end.

Noah Lapine, President

(Enclosure)

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 recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <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 print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

TransUnion P.O. Box 1000 Chester, PA 19016 1-800-916-8800 www.transunion.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Free Annual Report P.O. Box 105281 Atlanta, GA 30348 1-877-322-8228 annualcreditreport.com
---	---	--	---

Fraud Alert: You may want to 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>.

Security Freeze: Under U.S. law, you have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission 600 Pennsylvania Ave, NW Washington, DC 20580 consumer.ftc.gov , and www.ftc.gov/idtheft 1-877-438-4338	Maryland Attorney General 200 St. Paul Place Baltimore, MD 21202 oag.state.md.us 1-888-743-0023	North Carolina Attorney General 9001 Mail Service Center Raleigh, NC 27699 ncdoj.gov 1-877-566-7226	Rhode Island Attorney General 150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400
---	---	---	--

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information, as well as others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf