



LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

May 31, 2019

Via E-Mail

Gordon J. MacDonald, Attorney General
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
E-Mail: attorneygeneral@doj.nh.gov

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent LPR Construction (“LPR”) in connection with a recent data security incident described in greater detail below. LPR takes the security and privacy of all personal information within its control very seriously and has taken significant steps to bolster its security posture.

1. Nature of the security incident.

On March 6, 2019, LPR learned that an unauthorized individual had gained access to an email account belonging to one LPR employee. As soon as LPR learned of this information, LPR immediately began an investigation and took steps to secure all employee email accounts. In addition, LPR engaged an independent forensics firm to determine what happened and whether personal information had been impacted. On April 5, 2019, the forensics firm engaged to conduct the investigation determined that five additional accounts had been accessed as well. The forensics firm then confirmed that certain personal information was contained within these six email accounts. Upon identification of the individuals associated with that information, LPR immediately took steps to identify mailing addresses for all potentially impacted individuals, which was completed on May 24, 2019, in order to provide notification of this incident.

The information involved in this data security incident may have included the following: name, address, date of birth, Social Security number, driver’s license or state identification number, passport number, username and account passwords, tax information, digital signature, financial account information, health and/or medical information and/or health insurance information, mother’s maiden name, and birth and/or marriage certificate.

2. Number of New Hampshire residents affected.

A total of one (1) New Hampshire resident was affected by this incident. LPR is in the process of notifying the affected New Hampshire resident via the enclosed letter.

3. Steps taken relating to the incident.

Upon learning of this incident, LPR took the steps described above. LPR also updated its internal procedures and has implemented additional safeguards to help prevent a similar incident from occurring in the future.

LPR has no evidence to suggest that information contained within the email accounts at issue has been misused. Nonetheless, out of an abundance of caution, LPR has also offered impacted individuals one year of credit monitoring and identity protection services at no cost.

4. Contact information.

LPR is dedicated to protecting the sensitive information that is in its control. If you have any questions or need additional information, please do not hesitate to contact me at (720) 292-2052, or by e-mail at Alyssa.Watzman@LewisBrisbois.com.

Sincerely,

/s/ Alyssa R. Watzman

Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

ARW:ldg
Encl.: Consumer Notification Letter



C/O ID Experts
PO Box 4219
Everett WA 98204

ENDORSE



CARE OF
NAME
ADDRESS1
ADDRESS2
CSZ
COUNTRY

2Dcode
SEQ

BREAK

To Enroll, Please Call:

1-800-256-5855

Or Visit:

<https://ide.myidcare.com/lpr-enroll>

Enrollment Code: <<XXXXXXXXXX>>

May 31, 2019

Subject: Notice of Data Security Incident

Dear <<FirstName>> <<LastName>>,

We are writing to inform you of a data security incident that may have affected your personal information. At LPR Construction (“LPR”), we take the privacy and security of personal information very seriously and regret any concern that this incident may cause you. That is why we are informing you about the incident, offering you twelve (12) months of credit monitoring and identity protection services at no cost to you, and providing information to you about steps that can be taken to help protect your personal information.

What Happened? On March 6, 2019, LPR learned that an unauthorized individual may have gained access to email accounts belonging to some LPR employees. Some of the messages and attachments within those accounts contained your personal information. As soon as we learned of this information, we immediately began an investigation and took steps to secure all employee email accounts. We also engaged an independent forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization.

On May 10, 2019, we confirmed that your personal information was contained within an email account belonging to an employee of LPR that may have been accessed by an unauthorized individual. We then identified your mailing address on May 24, 2019 and immediately took steps to notify you of this incident.

LPR has no evidence to suggest that your personal information has been misused. Nonetheless, out of an abundance of caution, LPR has made arrangements to offer you credit monitoring and identity protection services for a period of twelve (12) months at no cost to you.

What Information Was Involved? The information involved in this incident may have included your name, address, date of birth, Social Security number, driver’s license or state identification number, passport number, username and account passwords, tax information, digital signature, financial account information, health and/or medical information and/or health insurance information, mother’s maiden name, and birth and/or marriage certificate.

What Are We Doing? Upon learning of this incident, LPR took the steps described above. We have also updated our internal procedures and have implemented additional safeguards to minimize the chance that an incident like this could occur in the future.

Although we have no evidence that your information has been misused, out of an abundance of caution, we are providing you with information about steps that you can take to help protect your personal information and we are offering you credit monitoring and identity protection services at no cost to you through ID Experts®, a leader in risk mitigation and response. These services include: twelve (12) months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, exclusive educational materials and fully managed identity theft recovery services. With this protection, ID Experts will help you to resolve issues if your identity is compromised.

To receive these services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file. The deadline to enroll in these services is August 31, 2019.

What You Can Do: You should follow the recommendations on the following page regarding steps you can take to help protect your personal information. We also encourage you to contact ID Experts with any questions and to enroll in the free services provided by calling 1-800-256-5855 or by going to <https://ide.myidcare.com/lpr-enroll> and using the Enrollment Code provided in this letter. ID Experts representatives are available to assist you Monday through Friday from 5 am - 5 pm Pacific Time.

We encourage you to take full advantage of this service offering. ID Experts representatives are fully versed on the incident and can answer questions or concerns you may have.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call ID Experts at 1-800-256-5855 Monday through Friday from 5 am – 5 pm Pacific Time, and please have your Enrollment Code ready.

We take the security of all information that we store in our systems very seriously. Please accept our sincere apologies and know that we deeply regret any worry or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'DAS', is positioned above the printed name of the sender.

Dana Hohn Strange
Director, HR

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:

Equifax P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285 www.equifax.com	Experian P.O. Box 9532 Allen, TX 75013 1-888-397-3742 www.experian.com	TransUnion P.O. Box 1000 Chester, PA 19016 1-877-322-8228 www.transunion.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 one year. 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: In some US states, you have the right to put a security freeze on your credit file. 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. A security freeze may be placed or lifted free of charge. 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, Federal Trade Commission or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission 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), including the right to know what is in your file, to dispute incomplete or inaccurate information, and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. 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.

