

Morgan Lewis

Ronald W. Del Sesto, Jr.
Stephany Fan
ronald.delsesto@morganlewis.com
stephany.fan@morganlewis.com

VIA FIRST CLASS MAIL

July 17, 2018

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

Re: Notification of Potential Security Breach

Dear Office of the Attorney General:

This Firm represents DSCI, LLC dba TPx Communications ("TPx") in connection with a situation where an unauthorized individual outside of the company may have gained access to the personal information of 11 New Hampshire residents.

On May 24, 2018, TPx discovered that one TPx employee had inadvertently sent an email with an attachment containing the personal information, including the first name, last name, address, birth date and social security number, of 23 total TPx employees to an errant email address on May 23, 2018.

Upon becoming aware of this incident, TPx has been and continues to take steps to secure its system. It has completed its investigation into the incident and instructed the employee how to avoid similar incidents from occurring in the future. In this particular case, the employee was attempting to send this information over TPx's internal, wired, secure intranet to another employee. TPx is also initiating additional employee training to ensure that all employees are following relevant procedures when transmitting such information both internally and externally.

Further information about what TPx has done and what it is recommending to the individuals is provided in a notification letter that TPx sent to the 11 New Hampshire residents affected on July 16, 2018.

RECEIVED

JUL 20 2018

CONSUMER PROTECTION

Morgan, Lewis & Bockius LLP

1111 Pennsylvania Avenue, NW
Washington, DC 20004
United States

📞 +1.202.739.3000
📠 +1.202.739.3001

Office of the Attorney General
July 17, 2018
Page 2

If you have any questions, please feel free to contact the undersigned.

Regards,



Ronald W. Del Sesto, Jr.
Stephany Fan

Counsel for *DSCI, LLC dba TPx Communications ("TPx")*

Enclosures



515 S. FLOWER STREET, 45TH FLOOR, LOS ANGELES, CA 90071 TPX.COM

July 16, 2018

[Name]
[Address]
[City, State Zip]

Notice of Data Breach

Dear [Name],

We value you and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that involves your personal information.

WHAT HAPPENED?

On May 23, 2018, an employee in our Human Relations Department inadvertently sent an email to an email address associated with an individual that is not a company employee. Attached to the email was a file that included your personal information.

WHAT INFORMATION WAS INVOLVED?

The file attached to the email included personally identifiable information. Specifically, your first name, last name, address, birth date and social security number were in the attachment.

WHAT WE ARE DOING

We respect your privacy and deeply regret that this incident occurred. We are reviewing our internal policies and procedures that address the transmission of this information and will implement additional employee training to make sure that all employees understand the risks and care needed when transmitting this information both internally and externally. We are also notifying relevant state agencies regarding the incident.

WHAT YOU CAN DO

Please also review below the [Steps You Can Take to Further Protect Your Information](#) for further information on steps you can take to protect your information, and how to receive free credit monitoring/identity theft protection services for two years.

FOR MORE INFORMATION

For further information and assistance, please contact Fran Schwartz, Director, Benefits and Compensation, Fran.Schwartz@TPx.com, 213-223-4228.

Sincerely,

Lisa Foley
Vice President, Human Resources

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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). 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**

We recommend that you 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 access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(800) 685-1111
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 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>.

- **Credit Report Monitoring and Identity Theft Protection Services - EXPERIAN**

In addition, we have arranged with Experian to provide you with credit monitoring/identity theft protection services for two years, at no cost to you.

To take advantage of this offer, you must enroll by October 31, 2018. Please review the Experian information below.

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. 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 offer is available to you for two years 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.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary two-year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Ensure that you enroll by: **October 31, 2018** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/3bplus>
- Provide your activation code:

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by **October 31, 2018**. Be prepared to provide engagement number **DB07792** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 2-year 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.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

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 for this information.

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

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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

We recommend that you review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Taking Charge: What to Do if Your Identity is Stolen, 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-taking-charge.pdf>.

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 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. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$5 to place, lift, or remove the security freeze.