MULLEN COUGHLIN LLC

James E. Prendergast
Office: 267-930-4798
Fax: 267-930-4771
Email: jprendergast@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 10, 2017

VIA U.S. 1st CLASS MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Foster:

We represent TransPerfect Global, Inc. ("TransPerfect"), 3 Park Avenue, 39th Floor, New York, New York 10016, and are writing to notify your office of an incident that may affect the security of personal information relating to nineteen (19) New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, TransPerfect does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On January 17, 2017, TransPerfect was the targeted victim of an email phishing attack by an individual pretending to be a TransPerfect senior executive. Through this attack, a request was made from what appeared to be the senior executive for employee information. Copies of W-2 forms generated by TransPerfect for 2015 and January 2017 payroll information relating to certain current employees were provided to the individual before it was discovered that the fraudulent request was made from a "spoofed" email. Since discovering that it had fallen victim of the scam, TransPerfect has been working tirelessly to investigate this incident, mitigate its impact, confirm the best address for all affected individuals, and provide notice to affected individuals.

Notice to New Hampshire Residents

On January 20, 2017, TransPerfect provided preliminary notice to current employees, and certain former employees if possible, via email. A copy of this notice is attached here as ***Exhibit A***. On February 8, 2017, TransPerfect began providing statutorily required written notice of this incident to all affected current and former employees, which includes nineteen (19) New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit B***. However, we note that the content of this notice varies slightly by individual recipient depending upon the types of their information determined to be impacted.

Other Steps Taken and to Be Taken

Upon discovering the fraudulent nature of the email, TransPerfect moved quickly to identify those that may be affected (including which types of information were impacted for each individual), to put in place resources to assist them, and to provide them with notice of this incident. Additionally, TransPerfect retained a third-party forensic investigator to determine the nature and scope of the incident and employee information impacted. While TransPerfect's investigation is ongoing, no employee, client, vendor or company information stored within TransPefect's systems has been found to be impacted outside of the particular employee information that was sent via email as a result of the email phishing attack.

TransPerfect is providing all potentially affected individuals access to 2 free years of credit and identity monitoring services, including identity restoration services, through Experian and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, TransPerfect is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud (where applicable), the contact details for Experian and for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

TransPerfect is also providing written notice of this incident to the major consumer reporting agencies and other state regulators as necessary. TransPerfect reported this incident to the FBI and local law enforcement. TransPerfect coordinated with the IRS and state tax authorities so that they can better monitor for tax-related fraud against individuals whose W-2 forms were impacted by this event.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4798.

Very truly yours,

James E. Prendergast of
MULLEN COUGHLIN LLC

JEP:ncl
Enclosures

Exhibit A

MEMORANDUM

TO: Team Members Employed by TransPerfect Global Inc. in 2015

DATE: January 20, 2017

RE: URGENT COMMUNICATION – Preliminary Notice of Data Incident

We recently discovered that our company was the targeted victim of an email spoofing attack on January 17, 2017, by an individual pretending to be one of our Chief Executive Officers. Through this attack, a request was made from what appeared to be the CEO for all 2015 TransPerfect employee W-2 information. Unfortunately, copies of all 2015 employee W2 forms were provided before we discovered that the request was made from a fraudulent account that appeared to be from one of our CEOs. We discovered the fraudulent nature of the request on January 17, 2017 and have since been working tirelessly to investigate and to mitigate the impact of the attack.

Additionally, a certain number of current employees' payroll information for the period ended on January 13, 2017, including name and direct deposit bank account number and routing number, was provided to the unknown individual as a result of this incident. We are currently investigating this issue further to confirm those employees impacted by this specific issue, and we will continue to provide updates as we learn more.

Please note that if your employment did not begin with TransPerfect until 2016, then your W2 information has not been impacted as a result of this incident.

The confidentiality, privacy, and security of our employee information is among our highest priorities. While our investigation is ongoing, we felt it important to notify you about this incident and what we are doing to investigate and respond as quickly as possible. Here are some actions that we are taking and that we encourage you to take:

- Identity Protection. As a precaution, for those individuals affected by this incident, we are arranging for an outside vendor to protect your identity at no cost to you. The cost of this service will be paid for by TransPerfect, and instructions for activating your protection will be included in a forthcoming communication. ***We strongly encourage you to act to take advantage of these free identity protection services as soon as possible after we provide the instructions for doing so.*** It will be incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

- Notice to Affected Individuals. We also will be mailing information to all impacted current and former TransPerfect team members as quickly as possible.

- Call Center for Employee Questions. We have established call center services to answer questions and concerns regarding this incident. We understand that you may have questions about this incident that are not addressed in this letter. Beginning at 4:30 PM Eastern today, if you have additional questions, please call our dedicated assistance line at **(877) 218-3036,** Monday through Saturday, 9 a.m. to 7 p.m. EST (Closed on U.S. observed holidays) and provide reference number **8617012017** when calling.

- Notice to Law Enforcement and the IRS. We immediately reported this incident to the NYPD and to federal law enforcement and are also notifying any necessary state regulators as well. We also are reporting this incident to the IRS so that they may immediately take steps to monitor for attempts to file fraudulent tax returns using TransPerfect employee information. The IRS may also take steps, as necessary, to notify appropriate state taxing authorities of the incident.

- Filing of 2016 Tax Returns. **We encourage you to file your 2016 tax return as soon as possible, beginning on Monday, January 23, 2017**. We understand that you may not have all necessary documents to file your 2016 tax return yet, but we encourage you to file an IRS Form 14039 (an identity theft affidavit) immediately via mail or fax. We have attached an IRS Form 14039 to this memo for your convenience, which contains instructions and a description of this incident. You can contact the IRS at http://www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

- **Our payroll provider, ADP, expects W2s to be available on the portal early next week with hard copies being mailed on or about the 31st of January.**

- Employee Training. Unfortunately, even the best technology cannot prevent all cyber-attacks, particularly those intended to fool employees into providing sensitive company information. We will continue and improve upon our information security awareness and training programs for all employees.

We apologize for any inconvenience this incident causes you. Please know that we are working diligently to remedy this incident and to prevent any similar incidents from occurring in the future. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at **(877) 218-3036, Monday** through Friday, 9 a.m. to 7 p.m. EST (Closed on U.S. observed holidays) and provide reference number **8617012017** when calling.

Exhibit B

TRANSPERFECT

123456

Return Mail Processing
P.O. Box 130
Claysburg, PA 16625-0130

##C5792-L03-0123456
123456 SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN US 12345-6789

February 10, 2017

Re: Notice of Data Breach

Dear Sample A Sample:

TransPerfect Global, Inc. ("TransPerfect") is writing to make you aware of a recent event that may affect the security of your personal information. If you are a current employee of TransPerfect or one of its subsidiaries or if we were able to identify a valid email address for you, we previously sent you email communications regarding this same incident. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information, should you feel it is appropriate to do so.

What Happened? Late on January 17, 2017, we discovered that our company was the targeted victim of an email phishing attack earlier that day by an individual pretending to be a senior executive. Through this attack, a request was made from what appeared to be Liz Elting (Co-CEO) for employee information. Copies of W-2 forms generated by TransPerfect for 2015 and January 2017 payroll information relating to certain current employees were provided to the individual before it was discovered that the fraudulent request was made from a "spoofed" email. Since discovering that we had fallen victim of the scam, we have been working tirelessly to investigate this incident, mitigate its impact, and provide notice to affected individuals.

What Information Was Involved? TransPerfect determined that a file containing (1) a copy of your IRS Tax Form W-2 generated by TransPerfect for 2015 and (2) January 2017 payroll information (including your name, address, employee identification number, direct deposit bank account number and routing number, and 2-week earnings amount) were sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) employee name; (2) employee address; (3) employee's Social Security number; and (4) the employee's wage information.

What We Are Doing. The confidentiality, privacy, and security of our current and former employees' information is one of our highest priorities. TransPerfect has stringent security measures in place to protect the security of information in our possession. At this time, we do not believe that the individuals who sent the fraudulent emails accessed our computer network or that our IT systems were otherwise compromised by this attack. However, our IT team, with assistance from IT forensics and cyber specialists, are assessing the security and soundness of our systems. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards, establish protocols for responding to email requests for sensitive information, and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. We have contacted the FBI, certain state tax authorities, local law enforcement, and relevant state Attorneys General. We also have coordinated with the IRS and state tax authorities so that they can better monitor for tax-related fraud against individuals impacted by this event.

As an added precaution, we have arranged to have Experian protect your identity for 24 months at no cost to you. The cost of this service will be paid for by TransPerfect. ***We strongly encourage you to act to take advantage of these free identity protection services as soon as possible.*** It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service. If you have already received an email from us regarding these services, please note that the below reflects that same offer.

While Fraud Resolution assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through ProtectMyID® Elite 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:

1. Ensure that you **enroll by**: February 10, 2019 (Your code will not work after this date.)
2. **Visit** the ProtectMyID website to enroll: **www.protectmyid.com/enroll**
3. Provide your **activation code**: **XXXXXXXXXX**

If you have questions about the incident, need assistance with fraud resolution that arose as a result of this incident or would like an alternative to enrolling in ProtectMyID online, please contact Experian's customer care team at 877-441-6943 by February 10, 2019. Be prepared to provide engagement number **PC106106** as proof of eligibility for the fraud resolution services by Experian.

Additional details regarding your 24-MONTH ProtectMyID Membership:

A credit card is **not** required for enrollment in ProtectMyID.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in ProtectMyID:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and TransUnion files for indicators of fraud.
- **Internet Scan:** Alerts you if your information is found on sites containing compromised data.
- **Address Change Alerts:** Alerts you of changes to your mailing address
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **$1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.
- **Lost Wallet Protection:** Get help replacing credit, debit, and medical insurance cards.

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.experian.com/fraudresolution for this information.

What You Can Do. You can review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud". You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 federal and state tax return as soon as possible. You can also monitor your impacted financial account for suspicious activity and change any passwords associated with that account.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at **(877) 218 - 3036** (toll free), Monday through Friday, 9:00 a.m. to 7:00 p.m. EST. Please provide reference number 8617012017 when calling.

123456

TransPerfect takes the privacy and security of the personal information in our care seriously. We sincerely regret any inconvenience or concern this incident has caused you.

Sincerely,

Andrea Green
Payroll Manager

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to file your 2016 federal and state tax return as soon as possible, if you have not already done so. If you have not already filed, we encourage you to file IRS Form 14039 with your 2016 tax return. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You should also look to the information made available by the tax authority for your state of residence and any other state where you file a tax return. For a list of websites for each US state's tax authority, visit http://www.taxadmin.org/state-tax-agencies.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and to change any passwords associate with accounts you believe may be impacted, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, list, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a

123456

freeze all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
1-800-685-1111	1-888-397-3742	1-888-909-8872
https://www.freeze.equifax.com	www.experian.com/freeze/	www.transunion.com/

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For Maryland residents**, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov. **For Rhode Island residents**, the Attorney General can be contacted by mail at 150 South Main Street, Providence, RI 02903; by phone at (401) 274-4400; and online at www.riag.ri.gov. A total of 4 Rhode Island residents may be impacted by this incident. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement. This notice was not delayed by a law enforcement investigation.