Holland & Knight

10 St. James Avenue | Boston, MA 02116 | T 617.523.2700 | F 617.523.6850
Holland & Knight LLP | www.hklaw.com

Scott T. Lashway
617-305-2119
scott.lashway@hklaw.com

September 27, 2018

**VIA EMAIL and U.S. MAIL**

Attorney General Gordon J. MacDonald
Office of the Attorney General
Consumer Protection and Antitrust Bureau
33 Capitol Street
Concord, NH 03301
*E-Mail: attorneygeneral@doj.nh.gov*

**Re: Notice Pursuant to New Hampshire Revised Statute § 359-C:20**

Dear Attorney General MacDonald:

Pursuant to New Hampshire Revised Statute § 359-C:20, we are writing on behalf of our client Tauck, Inc. ("Tauck") to notify you of a data security matter that occurred at a third-party benefit solutions provider, Progressive Benefit Solutions LLC ("PBS"), and which impacted a New Hampshire resident.

**Who This Impacted**

There was no compromise of Tauck's systems or infrastructure. However, we believe personal information of Tauck or Compass Employee Services, Inc. ("Compass") personnel and their dependents may have been compromised in connection with the data security matter at PBS. (Compass provides services of qualified personnel to Tauck in your state. Tauck has its principal place of business in Connecticut.) Specifically, based on information available to us from PBS, we believe that the information for approximately one (1) New Hampshire resident was impacted. Notification of this matter was mailed to the affected New Hampshire residents on or around September 13, 2018. A copy of this notification is attached as **Exhibit A**.

**What Happened**

1. February Email

Tauck is a travel services company located at 10 Westport Road, Wilton, Connecticut 06897. On February 1, 2018, a Tauck employee received an encrypted email, which Tauck believed was sent by PBS, containing information relating to certain participants in an employee benefit plan managed by PBS ("February Email"). We understand that PBS launched an investigation into the February Email and retained a third-party forensic firm to assist in that work. PBS subsequently confirmed that the February Email was sent, using PBS's email system, by an unauthorized party. On May 4, 2018, PBS disclosed to Tauck the results of their investigation.

As reported by PBS, PBS identified that, on February 1, 2018, an unauthorized actor accessed a PBS employee's email account and sent to certain other third parties an encrypted email containing information relating to participants in Tauck's or Compass's employee benefit plan. PBS confirmed that the unauthorized actor did not open the attachments to the February Email, and that there was no copying or removing of the attachments to the February Email, other than the February Email itself.

PBS further identified that two additional PBS employee email accounts were subject to unauthorized access dating back to January 15, 2018. PBS represented that it undertook a manual review of the inboxes of these two additional accounts. On or about May 17, 2018, PBS informed Tauck that their review of the two email accounts did not identify any additional information or personnel not already included in the February Email. According to PBS, PBS changed the credentials for the accounts within hours, thereby terminating the unauthorized actor's access; deactivated the link to access the encrypted February Email; instructed all recipients of the February Email to securely delete the email and attachments; and confirmed the recipients did not retain, forward, or otherwise misuse the information.

Based on the information available to Tauck from PBS at that time, Tauck believed that there was no evidence that any unauthorized third-party accessed or acquired the personal information of any Tauck or Compass personnel.

2. May Email

On or around May 24, 2018, Tauck received an email purporting to be from a PBS employee and attaching certain information regarding Tauck and Compass employees ("May Email"). Tauck immediately contacted PBS regarding the legitimacy of the email, and PBS indicated it was investigating the matter. On July 20, 2018, Tauck received a supplemental notice from PBS disclosing the results of their investigation into the May Email. PBS determined that the May Email had been sent from a "spoofed" email account that was made to look like it was coming from the PBS employee's account. Because the spoofed May Email did not originate from PBS's email account (i.e., was sent from an account external to PBS), PBS advised it was not possible to confirm all recipients of the May Email but that several recipients contacted PBS to inquire as to the May Email's legitimacy, including Tauck. PBS confirmed that, of those

individuals for whom PBS could confirm receipt, none read or saved the May Email and all deleted it upon PBS's request.

PBS recently confirmed that the information contained in the attachments to the spoofed May Email were identical to those attachments in the February Email.

Based on an evaluation of additional information reported by PBS to Tauck on or around August 13, 2018, we now have reason to believe that the data involved in the February Email may have been accessed or acquired by an authorized third party. At this time, we have no evidence to suggest that any misuse of impacted individuals' information has occurred as a result of this matter.

**What Information Was Involved**

The information contained in the attachments may have included the name, Social Security number, and date of birth of certain Tauck or Compass employees and, if applicable, their dependents. We have no evidence that any financial information, health insurance policy numbers, subscriber identification numbers, or any other unique health insurer identifier was at issue in this matter. There was no such information in the attachments.

**What We Are Doing**

Tauck takes the protection of personnel's personal information very seriously. As an added precaution, Tauck has arranged to provide thirty-six (36) months of triple bureau credit monitoring services to all impacted individuals at no charge to those individuals. Identity repair services are also being provided at no charge.

PBS has reported that in response to this data security matter it has taken steps to further enhance its security protocols. We are also in the process of evaluating and investigating this matter in order to prevent a similar occurrence in the future.

Below is the contact information for Philip Crosby, Chief Financial Officer:

Philip Crosby
Chief Financial Officer
Tauck, Inc.
10 Westport Road
Wilton, CT 06897
203-899-6850
pcrosby@tauck.com

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely yours,

Scott T. Lashway

# EXHIBIT A

COMPASS Employee Services, Inc.

10 Westport Road, B100 • Wilton, CT 06897
p: 203-899-6671 • f: 203-899-6612

[DATE]

[NAME]
[ADDRESS]

RE: Notice of Security Incident

Dear [NAME]:

We are writing to let you know about a data security matter, which we recently confirmed as having occurred on or about May 24, 2018 and February 1, 2018, involving a third party, Progressive Benefit Solutions LLC ("PBS"), with whom we contract to provide benefits services. You are receiving this letter because we believe your information may have been at issue in this matter.

**What Happened**

1. February Email

On February 1, 2018, a Tauck employee received an encrypted email that we believed was sent by PBS, but which PBS subsequently confirmed was sent by an unauthorized party, containing information relating to certain participants in Compass's employee benefit plan ("February Email"). We understand that PBS launched an investigation into the February Email and retained a third-party forensic firm to assist in that work. On May 4, 2018, PBS disclosed to Tauck*, by letter, the results of their investigation. PBS identified that, on February 1, 2018, an unauthorized actor accessed a PBS employee's email account and sent to certain other third parties an encrypted email containing information relating to participants in Compass's employee benefit plan. PBS confirmed that the unauthorized actor did not open the attachments to the February Email, and that there was no copying or removing of the attachments to the February Email, other than the February Email itself.

As a part of their investigation, PBS further identified that two additional PBS employee email accounts were subject to unauthorized access dating back to January 15, 2018. On or about May 17, 2018, PBS informed Tauck that the only Compass employee personal information in the two accounts were the attachments to the February Email. According to PBS, PBS changed the credentials for the accounts within hours, thereby terminating the unauthorized actor's access; deactivated the link to access the encrypted February Email; instructed all recipients of the

* Compass Employee Services' benefits are under the umbrella of Tauck Inc's benefit plan, all notification and investigation correspondence was sent to Tauck.

February Email to securely delete the email and attachments; and confirmed the recipients did not retain, forward, or otherwise misuse the information. **Based on PBS's reporting of their initial investigation, we believed that there was no evidence that any unauthorized third-party accessed or acquired Tauck employees' personal information.**

2. May Email

On or around May 24, 2018, Tauck received an email purporting to be from a PBS employee and attaching certain information regarding Compass employees ("May Email"). Tauck immediately contacted PBS regarding the legitimacy of the email, and PBS indicated it was investigating the matter. On July 20, 2018, PBS disclosed the initial results of their investigation into the May Email. PBS determined that the May Email had been sent from a "spoofed" email account, made to look like it was coming from a PBS email account, by an unauthorized third party. Because the spoofed May Email did not originate from PBS's email account, PBS advised it was not possible to confirm all recipients of the May Email, but that several recipients contacted PBS to inquire as to the May Email's legitimacy, including Tauck. PBS confirmed that, of those individuals for whom PBS could confirm receipt, none read or saved the May Email and all deleted it upon PBS's request.

PBS recently confirmed that the information contained in the attachments to the spoofed May Email were identical to those attachments in the February Email.

Based on additional information reported by PBS to Tauck on or around August 13, 2018, we now have reason to believe that the data involved in the February Email may have been accessed or acquired by an unauthorized third party. At this time, we have no evidence to suggest that any misuse has occurred as a result of this matter. In order to prevent and detect misuse of your information, we strongly encourage you to take preventative measures outlined in this letter.

**What Information Was Involved**

The information contained in the attachments may have included your and, if applicable, your dependents', name, Social Security number, and date of birth. We have no evidence that any financial information, health insurance policy numbers, subscriber identification numbers, or any other unique health insurer identifier was at issue in this matter. There was no such information in the attachments.

**What We Are Doing**

PBS has reported that in response to this data security matter it has taken steps to further enhance its security protocols. We are also in the process of evaluating and investigating this matter in order to prevent a similar occurrence in the future.

**What You Can Do**

We recommend that you enroll in the identity protection services we are offering, at no charge to you.

As an added precaution, we have arranged to have AllClear ID protect your identity for 36 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 36 months.

- AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call (866) 979-2595 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

- AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy (For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information). To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling (866) 979-2595 using the following redemption code: {RedemptionCode}.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

**For More Information**

There are additional actions you may consider taking to help protect your information. We have also provided resources where you can obtain additional information about identity theft and ways to protect yourself. Please refer to the final page of this letter for this information.

**Questions and Concerns**

We sincerely apologize that this occurred, regret any inconvenience it may cause you, and encourage you to take advantage of the product outlined herein. Should you have questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact Sharyn Cannon, Liz Malett or myself.

Sincerely,

Philip Crosby
Treasurer

## ADDITIONAL ACTIONS TO HELP REDUCE YOUR CHANCES OF IDENTITY THEFT

### ➢ PLACE A 90-DAY FRAUD ALERT ON YOUR CREDIT FILE

An **initial 90 day security alert** indicates to anyone requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the lender should take steps to verify that you have authorized the request. If the creditor cannot verify this, the request should not be satisfied. You may contact one of the credit reporting companies below for assistance.

| **Equifax** | **Experian** | **TransUnion** |
|---|---|---|
| PO Box 740241 | PO Box 4500 | PO Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19016 |
| 1-800-525-6285 | 1-888-397-3742 | 1-800-680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com |

### ➢ PLACE A SECURITY FREEZE ON YOUR CREDIT FILE

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a Security Freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process is also completed through each of the credit reporting companies.

### ➢ ORDER YOUR FREE ANNUAL CREDIT REPORTS

Visit www.annualcreditreport.com or call 877-322-8228.
Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

### ➢ MANAGE YOUR PERSONAL INFORMATION

Take steps such as: carrying only essential documents with you; being aware of whom you are sharing your personal information with and shredding receipts, statements, and other sensitive information.

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

- **USE TOOLS FROM CREDIT PROVIDERS**

Carefully review your credit reports and bank, credit card and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company.

- **BE ON THE LOOKOUT FOR PHISHING SCHEMES**

We recommend that you be on the lookout for suspicious emails. Specifically, be on the lookout for phishing schemes, which are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which is actually sent by a fraudulent impersonator.

Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (look for misspellings in the email address). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate.

- **OBTAIN MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF**

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

**Federal Trade Commission,** Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

**For Residents of Iowa**: You may also obtain information about preventing and avoiding identity theft from the Iowa Office of the Attorney General:

**Iowa Office of the Attorney General,** Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, 1-888-777-4590, consumer@ag.iowa.gov, https://www.iowaattorneygeneral.gov

**For residents of Maryland:** You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

**Maryland Office of the Attorney General,** Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

**For residents of Massachusetts:** You also have the right to obtain a police report.

**For residents of North Carolina:** You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

**North Carolina Attorney General's Office**, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

**For residents of Rhode Island:** You also have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General, Consumer Protection Unit
150 South Main Street, Providence, RI 02903, 1-401-274-4400,
http://www.riag.ri.gov/ConsumerProtection/About.php