October 13, 2023

New Hampshire Department of Justice
33 Capitol Street
Concord, NH 033301

By Email

RE: Taylored Services Parent Co.- Notice of Data Breach Incident

Attorney General Formella,

We are contacting you on behalf of our client, Taylored Services Parent Co. of Edison, New Jersey regarding a recent security incident at the company. Our client is in the process of notifying the individuals, which included one affected New Hampshire resident. A template of the letter being sent to the New Hampshire resident is attached for your review. Below is a summary of the incident.

On September 17, 2023, Taylored's information technology ("IT") systems were the target of a cybersecurity attack. Upon detecting the attack, Taylored's IT department worked quickly and diligently to contain and combat the attack. Taylored also promptly procured the services of cybersecurity specialists and security experts to assist in the investigation and mediation of the threat. During the initial days of our investigation, there was no indication that any unauthorized person accessed, copied, or removed information or data from Taylored's IT systems. However, on October 1st, while investigating a ransomware attack impacting the Taylored's systems, Taylored discovered that the personal information of certain employees and former employees of Taylored and former employees of entities acquired by Taylored through corporate transactions may have been compromised. Taylored discovered that the security of the personal data, including

Taylored responded promptly to sever any unauthorized access to such information.

Additionally, Taylored has continued to engage with cybersecurity specialists and security experts to review internal policies and processes and amending its security measures and protocols as needed. Taylored has also provided the affected individuals with credit monitoring services through Experian Information Solutions, Inc. at no charge to the individuals. Should you have any questions or concerns regarding this matter, please do not hesitate to contact me at

Sincerely,

Rachit Parikh

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 14, 2023

K1891-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

RE: Notice of Personal Information Data Breach. Please read this entire letter.

Dear Sample A. Sample:

We are contacting you regarding a data security incident involving Taylored Services Parent Co. Inc. ("Taylored") IT systems. The data security incident may affect current and former Taylored employees, as well as employees of entities purchased by Taylored via a corporate transaction ("Affected Individuals"). **You are among the Affected Individuals, and key data including .** Please fully read this letter and its attachments, which explain: the data breach incident; what we are doing to assist you in light of the data breach incident; and steps you can take to further protect yourself against possible identity theft.

We sincerely regret any inconvenience or concern caused by this incident. As detailed below, Taylored has purchased credit monitoring service on your behalf. Instructions are provided for registering for this service online. If you have further questions or concerns, or would like an alternative to enrolling online, please call toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number B106175.

If you have specific concerns, please call , extension 4, or email , and a Taylored representative will follow up as soon as possible.

Sincerely,

Matt Ennis
CEO

Taylored Services Parent Co. Inc.
201 Mill Road
Edison, NJ, 08837
W: www.tayloredservices.com

INFORMATION ABOUT THE DATA SECURITY BREACH AND HOW IT AFFECTS YOU

Why am I receiving this letter?	Because you are a current or former employee of Taylored (or a former employee of a company that Taylored previously acquired) and **your data has been identified at risk**. **Please take two actions: (1) sign up for credit monitoring services and (2) place a fraud alert on your credit files. Information on how to complete these two actions is detailed below.**
What Happened?	On September 17, 2023, Taylored's information technology ("IT") systems were the target of a cybersecurity attack. Upon detecting the attack, Taylored quickly and diligently worked to contain and combat the attack. During the initial days of our investigation, there was no indication that any unauthorized person accessed, copied, or removed information or data from Taylored's IT systems**. However, on October 1, 2023, Taylored was informed that a cyber threat actor may have gained access to electronic files that included personnel records including personal information (name, address, financial account information such as banking and payroll information, and/or social security numbers) of certain of our current and former employees.** We are contacting you to inform you of actions that Taylored is taking to remediate this situation and advise you on steps you can take to protect yourself against possible identity theft.
What Information is Involved?	**Our employee files include:**
How do I protect myself given this data breach risk?	As is fully described in this letter, we have purchased for you 24 months of credit monitoring services to help guard against identity theft. **We strongly encourage you to take advantage of this service. Please sign up for the credit monitoring services as soon as possible.**
What actions did Taylored take post breach incident?	We are fully reviewing and auditing our IT systems and security policies and procedures and will make any needed improvements and upgrades to better deter and protect against future cybersecurity incidents.
In addition to signing up for the Credit Monitoring Services, what else should I do?	**In addition to taking advantage of the credit monitoring service Taylored is providing to you, we recommend that you take the following actions**: **Place a fraud alert on your credit files as soon as possible**. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud ("credit hold"). When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A credit hold should not stop you from using your existing credit cards or other accounts. While a credit hold may delay your ability to obtain new lines of credit, it is highly likely to stop anyone else attempting to open a credit account in your name. An initial credit hold is valid for ninety (90) days. **To place a credit hold, contact one of the three major credit reporting agencies at the applicable telephone number, website, or mailing address listed below**. You only need to place the credit hold with one of the three agencies, that agency will notify the other two on your behalf. Once you have placed a credit hold, you will receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each agency. **Experian**: (888) 397-3742 www.experian.com or P.O. Box 2104, Allen, TX 75013 **Equifax:** (888) 766-0008 https://www.equifax.com/ P.O Box 740241, Atlanta, GA 30374 **TransUnion:** (800) 680-7289 www.transunion.com P.O. Box 2000, Chester, PA 19016

	When you receive a credit report from each agency, review the reports carefully to make sure you are not already the victim of identity theft. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report to discuss. You should also call your local police department and file a report for identity theft. Request a copy of the police report and store it in a secure location. You may need to provide a copy of the police report to creditors to correct your credit records or to access transaction records. Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in periodically reviewing your credit reports from the three major credit reporting agencies and in reviewing your financial account statements. You may obtain a free copy of your credit report once every by: 1. visiting *www.annualcreditreport.com* and completing a request for your credit report; 2. calling 877-322-8228 and requesting your credit report; or 3. by completing an Annual Credit Request Form at: *www.ftc.gov/bcp/menus/consumer/credit/rights.shtm* and mailing the form to: Annual Credit Report Request Service, P.O. Box 1025281 Atlanta, GA 30348-5283 For more information on identity theft, you may contact the Federal Trade Commission by visiting the website below or via the mail address or telephone number listed below: *www.ftc.gov/bcp/edu/microsites/idtheft/* Office of Policy and Coordination, Room CC5422 Bureau of Competition Federal Trade Commission 600 Pennsylvania Ave. N.W Washington, D.C. 20580 202-326-3300 If you received correspondence or any communication from the Internal Revenue Service that you may have been a victim of tax-related identity theft or that your tax filing was rejected as a duplicate, you should immediately fill out a Form 14039 Identity Theft Affidavit and submit it to the Internal Revenue Service. You should continue to file your tax return, as applicable, and attach the Form 14039 Identity Theft Affidavit to the return. Tax-related identity theft occurs when someone uses a taxpayer's stolen Social Security number to file a tax return claiming a fraudulent refund. You should also contact your state taxing authority if you have concerns that your tax filings are subject to fraud. For more information on when to file a Form 14039 Identity Theft Affidavit, you can visit the following IRS website: *https://www.irs.gov/newsroom/when-to-file-an-identity-theft-affidavit* For more information on tax-related identity theft, you can visit the following website: *https://www.irs.gov/newsroom/taxpayer-guide-to-identity-theft*

CREDIT MONITORING SERVICE

To help protect your identity, Taylored has paid the fees to permit you access to Experian IdentityWorks℠ for . This credit monitoring service is separate from the fraud alert you may put on your credit files, as explained above.

If you believe there was fraudulent use of your information as a result of this incident 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 from the date of the incident (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 Identity Restoration is available to you for 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.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 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:

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 . Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 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 file for indicators of fraud.
- **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.

---

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage.

ADDITIONAL STATE SPECIFIC INFORMATION

If you are a resident of Maryland:

- For more information on identity theft, you can visit or contact the Office of the Maryland Attorney General at the following:
    - Website: https://www.marylandattorneygeneral.gov/
    - Phone Number: 888-743-0023
    - Address: 200 St. Paul Place, Baltimore, MD 21202

If you are a resident of North Carolina:

- For more information on identity theft, you can visit or contact the Office of the North Carolina Attorney General at the following:
    - Website: https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-your-business-from-id-theft/security-breach-information/
    - Phone number: 919-716-6000
    - Address: 114 West Edenton Street, Raleigh, NC 27603

If you are a resident of New York:

- For more information on identity theft, you can visit the following websites:
    - New York Department of State Division of Consumer Protection https://dos.nysits.acsitefactory.com/consumer-protection
    - NYS Attorney General at: http://www.ag.ny.gov/home.html
    - Phone Number: 800-771-7755

If you are a resident of Washington, D.C.

- For more information on identity theft, you can visit or contact the Office of the Washington, D.C. Attorney General at the following:
    - Website: https://oag.dc.gov/
    - Phone Number: 202-727-3400
    - Address: 400 6th Street, NW, Washington, DC 20001