



[Return Address Line 1]
[Return Address Line 2]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

[Date]

RE: Important Security Notification. Please read this entire letter.

To the Estate of [First Name] [Last Name]:

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"). We are not aware of any actual identity theft as of the date of this notification however **your relative was among the Affected Individuals, and key data including their Social Security Number and Banking Data may be exposed. We sincerely regret any inconvenience or concern caused by this incident. 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 the personal information of your relative.**

If you have specific concerns, please call (732)-750-9000, extension 4 (HR), Option 5 (other inquiries) or email cyber.inquiry@tpservices.com, and a Taylored representative will follow up as soon as possible.

Sincerely,

A handwritten signature in cursive script that reads 'Matt Ennis'.

Matt Ennis
CEO

Taylored Services
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 your relative was a former employee of Taylored (or a former employee of a company that Taylored previously acquired) and <u>their data has been identified at risk.</u>
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 24, 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 the Personal Data of your relative.
What Information is Involved?	Our employee files include: their name, address, date of birth, financial account information such as payroll and banking information and/or social security number (“Personal Data”).
How do I protect the information of my relative given this data breach risk?	Please read the <i>Protecting Deceased Individuals</i> attachment and please contact the important agencies as suggested in the attachment.
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.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, please call [Experian TFN] 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 [B#####].

If your relative was 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 your relative is 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.acsifactory.com/consumer-protection>
 - NYS Attorney General at: <http://www.ag.ny.gov/home.html>
 - Phone Number: 800-771-7755

Protecting Deceased Individuals

Experian has collaborated with the Identity Theft Resource Center (ITRC) to provide information on steps you can take when a deceased or incapacitated loved one is affected by a data compromise incident.

Deceased

Decrease the risk of their identity theft regardless of age by following these steps:

- 1) Obtain at least multiple copies of the official death certificate when it becomes available. In some cases, you will be able to use a photocopy, but some businesses will request an original death certificate. Since many death records are public, a business may require more than just a death certificate as proof.
- 2) If there is a surviving spouse or other joint account holders, make sure to immediately notify relevant credit card companies, banks, stockbrokers, loan/lien holders, and mortgage companies of the death. They may require a copy of the death certificate to do this, as well as permission from the survivor, or other authorized account holders.
- 3) The executor or surviving spouse will need to discuss all outstanding debts and how they will be dealt with. You will need to transfer the account to another person or close the account. If you close the account, ask them to list it as: "Closed. Account holder is deceased."
- 4) Contact all CRAs (**see contact information below**), credit issuers, collection agencies, and any other financial institution that need to know of the death using the required procedures for each one. The following are general tips:
 - a. Include the following information in all letters:
 - i. Name and SSN of deceased
 - ii. Last known address
 - iii. Last 5 years of addresses
 - iv. Date of birth
 - v. Date of death
 - vi. To speed up processing, include all requested documentation specific to that agency in the first letter
 - b. Send the appropriate Court signed Executive papers
 - c. Send all mail certified, return receipt requested.
 - d. Keep copies of all correspondence, noting date sent and any response(s) you receive.
 - e. Request a copy of the decedent's credit report - See sample template below. A review of each report will let you know of any active credit accounts that still need to be closed, or any pending collection notices. Be sure to ask for all contact information on accounts currently open in the name of the deceased (credit granters, collection agencies, etc.) so that you can follow through with those entities.
 - f. Request that the report is flagged with the following alert: "Deceased. **Do not** issue credit. If an application is made for credit, notify the following person(s) immediately: (list the next surviving relative, executor/trustee of the estate and/or local law enforcement agency- noting the relationship)."

Note: Friends, neighbors or distant relatives do not have the same rights as a spouse or executor of the estate. They are classified as a third party and a CRA may not mail out a credit report or change data on a consumer file upon their request. If you fall into this classification and are dealing with a very unique situation, you may write to the CRA and explain the situation. They are handled on a case-by-case basis. You may also apply to the courts to be named as an executor of the estate.

Other groups to notify:

- Social Security Administration
- Insurance companies - auto, health, life, etc.
- Veteran's Administration - if the person was a former member of the military



- Immigration Services - if the decedent is not a U.S. citizen
- Department of Motor Vehicles if the person had a driver's license or state ID card. Also make sure that any vehicle registration papers are transferred to the new owners
- Agencies that may be involved due to professional licenses - bar association, medical licenses, cosmetician, etc.
- Any membership programs- video rental, public library, fitness club, etc.

Specific Credit Reporting Agencies (CRAs) information for ordering a credit report or place a deceased flag:

Experian (888) 397-3742 www.experian.com or P.O. Box 2104, Allen, TX 75013	
<p><u>To order a credit report:</u></p> <p>A spouse can obtain a credit report by simply making the request through the regular channels - mail, phone and Internet. The spouse is legally entitled to the report.</p> <p>The executor of the estate can obtain a credit report but must write Experian with a specific request, a copy of the executor paperwork and the death certificate.</p>	<p><u>For requests or changes:</u></p> <p>A spouse or executor may change the file to show the person as deceased via written request. A copy of the death certificate and in the case of the executor, the executor's paperwork must be included with the request.</p> <p>After any changes, Experian will send an updated credit report to the spouse or executor for confirmation that a deceased statement has been added to the credit report. This is important as executors and spouse can request other types of "changes" that we may not be able to honor.</p> <p>If identity theft is a stated concern, Experian will add a security alert after the file has been changed to reflect the person as deceased.</p> <p>If there are additional concerns, Experian will add a general statement to the file at the direction of the spouse/executor. The spouse/executor must state specifically what they want the general statement to say, such as "Do not issue credit."</p>
Equifax: (888) 766-0008 https://www.equifax.com/ P.O. Box 740241, Atlanta, GA 30374	
<p><u>To order a credit report:</u></p> <p>Equifax requests that the spouse, attorney or executor of the estate submit a written request to receive a copy of the deceased consumer's' file. The request should include the following:</p> <p>A copy of a notarized document stating that the requestor is authorized to handle the deceased consumer's affairs (i.e.: Order from a Probate Court or Letter of Testamentary)</p>	<p><u>For requests or changes:</u></p> <p>Equifax requests that a spouse, attorney or executor of the estate submit a written request if they would like to place a deceased indicator on the deceased consumer's file. The written request should include a copy of the consumer's death certificate. The request should be sent to the address listed above.</p> <p>Upon receipt of the death certificate, Equifax will attempt to locate a file for the deceased consumer and place a death notice on the consumer's file. In addition, Equifax will place a seven year promotional block on the deceased consumer's file. Once Equifax's research is complete, they will send a response back to the spouse, attorney, or executor of the estate.</p>



TransUnion: (800) 680-7289 www.transunion.com P.O. Box 2000, Chester, PA 19016	
<p><u>To order a credit report:</u></p> <p>TransUnion requires proof of a power of attorney, executor of estate, conservatorship or other legal document giving the requestor the legal right to obtain a copy of the decedent’s credit file.</p> <p>If the requestor was married to the deceased and the address for which the credit file is being mailed to is contained on the decedent’s credit file, then TransUnion will mail a credit file to the surviving spouse.</p> <p>If the deceased is a minor child of the requestor, TransUnion will mail a credit file to the parent upon receipt of a copy of the birth certificate or death certificate naming the parent as requestor.</p>	<p><u>For requests or changes:</u></p> <p>Placing a “decease alert” on reports: TransUnion will accept a request to place a temporary alert on the credit file of a deceased individual from any consumer who makes such a request and identifies themselves as having a right to do so. The requestor’s phone number is added to the temporary, three month alert. Upon receipt of a verifiable death certificate, TransUnion will entirely suppress the decedent’s credit file and so note it as a deceased consumer.</p> <p>TransUnion will not mail out a copy of its contents without the requirements mentioned above.</p> <p>If you suspect fraud, TransUnion suggests a call to their fraud unit at 800-680-7289. It will place the temporary alert over the phone and advise the requestor of what needs to be sent to suppress the credit file and to disclose a copy of its contents. Requests can also be emailed to fvad@transunion.com.</p>

When you receive a credit report from each agency, review the reports carefully to make sure your relative is not already the victim of identity theft. Look for accounts they did not open, inquiries from creditors that they did not initiate, and confirm that their personal information, such as previous 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 their credit records or to access transaction records.

Even if you do not find signs of fraud on their 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 their credit report as described above.

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 they 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 their 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>