



Rachit Parikh
71 South Wacker Drive, Suite 1600
Chicago, IL 60606
Direct Dial: 312.212.4966
rparikh@beneschlaw.com

October 13, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

RE: Notice to the Office of the Maryland Attorney General of Data Breach Incident

Attorney General Brown

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 5 affected Maryland residents. A template of the letter being sent to Maryland residents 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 name; address; financial account information, including payroll and banking information; and/or social security number may have been compromised. 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 312-212-4966 or rparikh@beneschlaw.com

Sincerely,

/Rachit Parikh/

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 your Social Security Number and Banking Data may be exposed.** 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 833-420-2822 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 (732)-750-4000, extension 4, or email cyber.inquiry@tpservices.com, and a Taylored representative will follow up as soon as possible.

Sincerely,

Matt Ennis

Matt Ennis
CEO

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

0000001



B106175

K1891-L01

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 <u>your data has been identified at risk</u> . 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: <u>your</u> 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 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. <u>Experian:</u> (888) 397-3742 www.experian.com or P.O. Box 2104, Allen, TX 75013 <u>Equifax:</u> (888) 766-0008 https://www.equifax.com/ P.O. Box 740241, Atlanta, GA 30374 <u>TransUnion:</u> (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 12 months 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 IdentityWorksSM for 24 months. 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 24 months 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 2 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** January 31, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code**: **ABCDEFGHI**

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 833-420-2822 by January 31, 2024. Be prepared to provide engagement number B106175 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24 MONTH 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 ExtendCARETM:** 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





Rachit Parikh
71 South Wacker Drive, Suite 1600
Chicago, IL 60606
Direct Dial: 312.212.4966
rparikh@beneschlaw.com

November 6, 2023

Maryland Attorney General's Office
Attn: Security Breach Notification

RE: Notice to the Office of the Maryland Attorney General of Data Breach Incident

Attorney General Andrea Joy Campbell:

This letter is an update for a data breach we reported to your office on October 13, 2023, on behalf of our client, Taylored Services Parent Co. of Edison, New Jersey. On October 14, 2023, Taylored notified all affected individuals at the addresses Taylored has on file. To ensure all affected individuals were notified, Taylored at the same time engaged Experian Consumer Services to verify and/or update the addresses Taylored has on file.

Based on address information Taylored has on file, 5 individuals were initially identified as residents of Maryland. On October 16, 2023, Taylored received the first set of results from Experian for updated addresses and learned that 2 additional individuals were now residing in Maryland. We sent a second notification of the breach to those all affected individuals on October 27, 2023. Concurrently, Taylored continued to investigate the breach and on October 23, 2023, Taylored discovered additional individuals who were affected. Taylored again engaged Experian to verify and/or update those addresses. On October 30th, 2023, as a result of the engagement with Experian, Taylored learned that an additional 3 individuals from Maryland were affected. Taylored is working to provide the 5 additional affected individuals with notice as soon as possible.

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 is providing all affected individuals, including the Maryland residents, with credit monitoring services through Experian Consumer Services at no charge to the individuals.

Should you have any questions or concerns regarding this matter, please do not hesitate to contact me at 312-212-4966 or rparikh@beneschlaw.com

Sincerely,

/Rachit Parikh/

Rachit Parikh

BENESCH, FRIEDLANDER, COPLAN & ARONOFF LLP



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

[Date]

RE: Notice of Personal Information Data Breach.

Please read this entire letter.

Dear [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 **you are among the Affected Individuals, and key data including your Social Security Number and Banking Data may have been exposed.**

We sincerely regret any inconvenience or concern caused by this incident. As detailed below and in order to mitigate the risk of identity theft, Taylored has purchased credit monitoring service from Experian on your behalf. Instructions for registering for this service online or over the phone are provided below under the "**Credit Monitoring**" section. Please take the following three key actions, as more fully explained in the attached program guides:

- (1) Get a Free Copy of your Personal Credit Report by contacting www.annualcreditreport.com or calling 877-322-8228.
- (2) Sign up for the free Experian Credit Monitoring Services by following the instructions below, and
- (3) Place a fraud alert/ and or credit hold on your credit files (discuss these options with your Experian credit advisory).

Please note that in order to sign up for Experian Credit Monitoring Services, **you will need to verify your identity by answering correctly some key information shown in your Personal Credit Report.** Therefore, please be sure to get your free Personal Credit Report and review it **before** you contact Experian.

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

Sincerely,

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 you are a current or former employee of Taylored (or a former employee of a company that Taylored previously acquired) and <u>your data has been identified at risk.</u>
What do I need to do?	We are not aware of any actual identity theft as of the date of this notification however we highly recommend taking three actions: (1) Get a Free Copy of your Personal Credit Report by contacting www.annualcreditreport.com or calling 877-322-8228 (2) sign up for credit monitoring services by following the instructions below and (3) place a fraud alert/ and or credit hold on your credit files (discuss these options with your Experian credit advisory). Please note that in order to sign up for Experian Credit Monitoring Services, <u>you will need to verify your identity by answering correctly some key information shown in your Personal Credit Report.</u> Therefore, please be sure to get your free Personal Credit Report and review it <u>before</u> you contact Experian.
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. On October 24, 2023, Taylored discovered that your electronic files which may have been accessed and the files may have 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: <u>your</u> 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 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. <u>Experian:</u>

(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 12 months 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>



	You have a right to a Security Freeze prevents most potential creditors from viewing your credit reports and therefore, further restricts the opening of unauthorized accounts. 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. A separate Security Freeze must be requested and placed on the applicable 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. There is no charge to request a security freeze or to remove a Security Freeze.
--	---



CREDIT MONITORING SERVICE

To help protect your identity, Taylored has paid the fees to permit you access to Experian IdentityWorksSM for [Length of Service] months. 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 [Length of Service] months 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 [Length of Service] 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** [Enrollment End Date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Enrollment URL]
- Provide your **activation code:** [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 [Experian TFN] by [Enrollment End Date]. Be prepared to provide engagement number [B#####] as proof of eligibility for the Identity Restoration services by Experian. **Additionally, as part of the enrollment process, you may be asked a series of questions related to your past addresses or your financial information, for example banks you may use or the amount of your mortgage. These questions are to verify your identity as these services do share very sensitive information. We highly recommend that you obtain your free credit report, using the instructions above, prior to signing up.**

ADDITIONAL DETAILS REGARDING YOUR [LENGTH OF SERVICE] MONTH 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 ExtendCARETM:** 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.acsifactory.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 Rhode Island:

- For more information on identity theft, you can visit the following websites:
 - Rhode Island Attorney General at: <https://riag.ri.gov/>
 - Phone Number: 401-274-4400
 - Address: 150 South Main Street, Providence, RI 02903

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



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

October 26, 2023

K2347-L03-0000003 T00001 P001 *****SCH 5-DIGIT 12345

TO THE ESTATE OF
SAMPLE A SAMPLE - L03 DECEASED
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



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

To the Estate of 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"). 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.**

In an effort to promptly contact Affected Individuals, we sent an initial letter to the address that we had on file for the deceased. Since then, we have cross-checked all addresses through Experian. As a result of the cross-checking we learned that your relative was deceased. We extend our condolences. We also would like to notify you that as a result of the cross-checking for updated addresses this may be the first letter sent addressed to your relative. If this is the second letter that you are receiving, please disregard the initial letter.

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

Sincerely,

Matt Ennis

Matt Ennis
CEO

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

0000003



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 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 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 **833-420-2822** 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 **B107656**.

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.acsitefactory.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

To order a credit report:

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.

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.

For requests or changes:

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.

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.

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.

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."

Equifax:
(888) 766-0008
<https://www.equifax.com/>
P.O. Box 740241, Atlanta, GA 30374

To order a credit report:

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:

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)

For requests or changes:

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.

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.

TransUnion: (800) 680-7289 www.transunion.com P.O. Box 2000, Chester, PA 19016	
<u>To order a credit report:</u> 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. 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. 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.	<u>For requests or changes:</u> 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. TransUnion will not mail out a copy of its contents without the requirements mentioned above. 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 .

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>





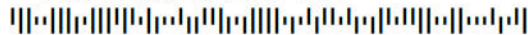
Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

October 26, 2023

K2347-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"). We are not aware of any actual identity theft as of the date of this notification however **you are among the Affected Individuals, and key data including your Social Security Number and Banking Data may have been exposed.**

We sincerely regret any inconvenience or concern caused by this incident. As detailed below and in order to mitigate the risk of identity theft, Taylored has purchased credit monitoring service from Experian on your behalf. Instructions for registering for this service online or over the phone are provided below under the "**Credit Monitoring**" section. Please take the following three key actions, as more fully explained in the attached program guides:

- (1) Get a Free Copy of your Personal Credit Report by contacting www.annualcreditreport.com or calling 877-322-8228.
- (2) Sign up for the free Experian Credit Monitoring Services by following the instructions below, and
- (3) Place a fraud alert/ and or credit hold on your credit files (discuss these options with your Experian credit advisory).

Please note that in order to sign up for Experian Credit Monitoring Services, **you will need to verify your identity by answering correctly some key information shown in your Personal Credit Report.** Therefore, please be sure to get your free Personal Credit Report and review it **before** you contact Experian.

In an effort to promptly contact Affected Individuals, we sent an initial letter to the address that we had on file for you. Since then we have cross-checked all addresses through Experian. As a result, this may be the first letter you are receiving. If this is the second letter you have received, it serves as an update to the initial letter. Please review this letter in detail as it does contain updated instructions compared to the initial letter.

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

Sincerely,

Matt Ennis

Matt Ennis, CEO
Taylored Services
201 Mill Road
Edison, NJ, 08837
W: www.tayloredservices.com

0000001



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 <u>your data has been identified at risk.</u>
What do I need to do?	We are not aware of any actual identity theft as of the date of this notification however we highly recommend taking three actions: (1) Get a Free Copy of your Personal Credit Report by contacting www.annualcreditreport.com or calling 877-322-8228 (2) sign up for credit monitoring services by following the instructions below and (3) place a fraud alert/ and or credit hold on your credit files (discuss these options with your Experian credit advisory). Please note that in order to sign up for Experian Credit Monitoring Services, <u>you will need to verify your identity by answering correctly some key information shown in your Personal Credit Report.</u> Therefore, please be sure to get your free Personal Credit Report and review it <u>before</u> you contact Experian.
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: <u>your</u> 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 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. <u>Experian:</u> (888) 397-3742 www.experian.com or P.O. Box 2104, Allen, TX 75013 <u>Equifax:</u> (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 12 months 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 IdentityWorksSM for 24 months. 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 24 months 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 24 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 January 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/credit
- Provide your **activation code: ABCDEFGHI**

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 **833-420-2822** by January 31, 2024. Be prepared to provide engagement number **B107655** as proof of eligibility for the Identity Restoration services by Experian. **Additionally, as part of the enrollment process, you may be asked a series of questions related to your past addresses or your financial information, for example banks you may use or the amount of your mortgage. These questions are to verify your identity as these services do share very sensitive information. We highly recommend that you obtain your free credit report, using the instructions above, prior to signing up.**

ADDITIONAL DETAILS REGARDING YOUR 24 MONTH 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 ExtendCARETM:** 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





[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@tps-services.com, and a Taylored representative will follow up as soon as possible.

Sincerely,

A handwritten signature in black ink 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.acsitefactory.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	
<u>To order a credit report:</u> 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. 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.	<u>For requests or changes:</u> 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. 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. 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. 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."
Equifax: (888) 766-0008 https://www.equifax.com/ P.O. Box 740241, Atlanta, GA 30374	
<u>To order a credit report:</u> 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: 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)	<u>For requests or changes:</u> 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. 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.

TransUnion: (800) 680-7289 www.transunion.com P.O. Box 2000, Chester, PA 19016	
<u>To order a credit report:</u> 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. 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. 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.	<u>For requests or changes:</u> 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. TransUnion will not mail out a copy of its contents without the requirements mentioned above. 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 .

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>