

VIA EMAIL

Office of the Attorney General, Maryland
Attn: Security Breach Notification

To Whom it May Concern:

Perennials and Sutherland, LLC experienced a cyber attack by a sophisticated cyber hacking group. We have learned that on December 3, 2021, malware was introduced into our system via a phishing email. On December 5, 2021, we became aware that a significant portion of our systems had been encrypted and that certain stored files and data were likely copied from our network. We successfully locked the hacking group out the day they were discovered, December 5, 2021. Through the forensic investigation, we have now learned that the cyber criminals obtained some of our sensitive files during the attack.

After securely recovering the affected data, we reviewed that data to identify affected individuals. The affected individuals consist of current employees and former employees, as well as some of their beneficiaries and dependents. We then retained a third-party vendor to determine the current residencies of the affected individuals. Based on the address information we received from our vendor on January 7, 2022, we were informed that two Maryland residents were affected.

A copy of the sample breach letter that will be sent to the residents is attached. The actual letter will be mailed no later than January 20, 2022.

Files obtained contained Perennials and Sutherland, LLC's HR compliance information which may have included the name, Social Security Number, ID numbers (e.g., drivers' license numbers, passport numbers, or other government issued identification number), medical information provided to HR for purposes such as medical leave of absence or workers compensation, date of birth, or other types of employment-related information.

In response to these events, we immediately engaged a leading cybersecurity service provider to help with the investigation and remediation of the incident and to help mitigate the possibility of future incidents. We also have notified law enforcement of the attack. Notification has not been delayed due to a law enforcement investigation. To protect your information going forward, we have required that all user passwords be changed and have implemented several new security measures for monitoring and detection of threats to our

information systems. We are committed to improving our security practices and increasing cyber awareness education.

Please reach out to me at lsnyder@davidsutherlandinc.com if you have any further questions.

Laura Snyder, CFO
214.379.6443

date

address

address

NOTICE OF DATA BREACH

Dear addressee,

We are writing to notify you that Perennials and Sutherland, LLC experienced a security incident that involves your personal information.

What Happened? We experienced a cyber attack by a sophisticated cyber hacking group. We have learned that on December 3, 2021, malware was introduced into our system via a phishing email. On December 5, 2021, we became aware that a significant portion of our systems had been encrypted and that certain stored files and data were potentially copied from our network. We successfully locked the hacking group out the day they were discovered, December 5, 2021. Through the forensic investigation, we have now learned that the cyber criminals obtained some of our sensitive files during the attack.

What Information Was Involved? Files obtained contained Perennials and Sutherland, LLC's HR compliance information which may have included your name, Social Security Number, ID numbers (e.g., drivers' license numbers, passport numbers, or other government issued identification number), medical information provided to HR for purposes such as medical leave of absence or workers compensation, date of birth, or other types of employment-related information. Additionally, the name, date of birth, and social security number for the dependent(s) listed on your medical plan and name and social security number for life insurance beneficiaries may have been included in the files potentially exposed during the attack.

What Are We Doing? In response to these events, we immediately engaged a leading cybersecurity service provider to help with the investigation and remediation of the incident and to help mitigate the possibility of future incidents. We also have notified law enforcement of the attack. Notification has not been delayed due to a law enforcement investigation. To protect your information going forward, we have required that all user passwords be changed and have implemented several new security measures for monitoring and detection of threats to our information systems. We are committed to improving our security practices and increasing cyber awareness education.

We take our obligation to safeguard personal information very seriously and thus, we have arranged to have Experian IdentityWorksSM protect your identity for 24 months at no cost to you. We encourage you to enroll yourself in this service. Attachment A provides an overview of Experian IdentityWorksSM and how to enroll. If you have further questions or concerns, or would like an alternative to enrolling online, 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 [DB#####].

What Can You Do? Please review the “Further Steps and Contact List” information on the reverse side of this letter which identifies additional steps to take to protect your information. If you have additional questions or concerns about this incident, please email our human resources department at HR@davidsutherlandinc.com or contact Jennifer Hirz at (214) 379-6460.

We deeply regret that this incident occurred and any inconvenience this may cause you; and we thank you for your understanding. We will **NOT** send you any electronic communications regarding this incident and ask you to disclose any personal information.

Sincerely,

Laura Snyder
Chief Financial Officer

FURTHER STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION AND CONTACT LIST

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact each one of the three national credit reporting agencies (contact information below).

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: A security freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order 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. Under federal law, you may not be charged to place or remove a credit freeze.

Police Report: If you file a police report, you have the right to obtain a copy of it.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, FTC (<https://www.identitytheft.gov/>) or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. You may want to contact your state Attorney General to obtain further information. Below is the contact information for the Attorneys General for residents of New York, North Carolina, Rhode Island, Oregon, the District of Columbia, and Maryland.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Oregon Attorney General
100 SW Market Street
First Floor
Tilikum Room
Portland, OR 97201
help@oregonconsumer.gov

New York Attorney General
Office of the Attorney
General
The Capitol
Albany, NY 12224-0341
<https://ag.ny.gov/>
1-800-771-7755

**Office of the Attorney
General for the District of
Columbia**
400 6th Street NW
Washington, D.C. 20001
oag@dc.gov
<https://oag.dc.gov/>

**North Carolina
Attorney General**
9001 Mail Service
Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
<https://www.marylandattorneygeneral.gov/>
Main number: 410-576-6300
Toll-free: 1-888-743-0023
Consumer Hotline: 410-528-8662

**Rhode Island
Attorney General**
150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
401-274-4400

Contact Information for Credit Reporting Agencies:

	Equifax	Experian	TransUnion
To obtain a copy of your credit report	P.O. Box 740241 Atlanta, GA 30374 (866) 349-5191 www.equifax.com	P.O. Box 4500 Allen, TX 75013 (888) 397-3742 www.experian.com	P.O. Box 1000 Chester, PA 19016 (800) 888-4213 www.transunion.com
To obtain a security freeze	PO Box 105788 Atlanta, GA 30348 (800) 685-1111 www.equifax.com/personal/credit-report-services	PO Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 (888) 909-8872 www.transunion.com/credit-freeze
To place a fraud alert	P.O. Box 105069 Atlanta, GA 30348 (888) 766-0008 www.equifax.com/personal/credit-report-services	P.O. Box 2002 Allen, TX 75013 (888) 397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 (800) 680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert

Attachment A

Experian IdentityWorksSM

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.

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 will be 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 month 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 [DB#####] 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. Coverage may not be available in all jurisdictions.