McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

P 1.248.646.5070
F 1.248.646.5075

Heather Shumaker
Direct Dial: 248.402.4066
E-mail: hshumaker@mcdonaldhopkins.com

January 6, 2025

VIA EMAIL (Idtheft@oag.state.md.us)

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

Re: Sundance Holdings Group, LLC – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Sundance Holdings Group, LLC ("Sundance"), located at 3865 W 2400 S, Salt Lake City, UT 84120, regarding a recent security incident. I am writing to provide notification of an incident at Sundance that may affect the security of personal information of approximately one (1) Maryland resident. By providing this notice, Sundance does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On or about October 11, 2024, Sundance experienced unauthorized actor access to its network. Upon learning of this issue, Sundance promptly commenced a thorough investigation. As part of its investigation, Sundance has been working very closely with external cybersecurity professionals experienced in handling these types of incidents. After an extensive forensic investigation, Sundance discovered on December 16, 2024 that the impacted systems, which were accessed on October 11, 2024, contained some personal information for one (1) Maryland resident. The impacted information for the Maryland resident potentially includes the individual's name, date of birth, driver's license number, social security number, passport number, green card information, bank account number, and health insurance information including information related to health issues, diagnoses, and dependent information.

To date, Sundance is not aware of any reports of identity fraud or financial fraud for any information as a direct result of this incident. Nevertheless, out of an abundance of caution, Sundance wanted to inform you (and the affected resident) of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Sundance is providing the affected resident with notification of this incident, commencing on January 6, 2025. The notice will be in substantially the same form as the letter attached hereto. Sundance is also offering the affected resident complimentary credit monitoring services. Sundance is advising the affected resident to always remain vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity on a regular basis. Sundance is also advising the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. Additionally, the affected resident is being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission and the Maryland Attorney General.

At Sundance, protecting the privacy of personal information is a top priority. Sundance is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Further, Sundance continues to evaluate and improve, where appropriate, it's administrative and technical safeguards including its policies, procedures, protocols, and tools to protect its network environment.

If you have any additional questions, please contact me at (248) 402-4066 or hshumaker@mcdonaldhopkins.com.

Very truly yours,

Heather Shumaker

Encl.

McDonald Hopkins
A business advisory and advocacy law firm®

Sundance Holdings Group
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

sundance

[redacted]

000010102G0500

P

[redacted]

Dear [redacted]:

The privacy and security of the personal information entrusted to us is of the upmost importance to Sundance Holdings Group, LLC ("Sundance"). We are writing to provide you with information regarding a recent cybersecurity incident that potentially involved some of your personal information. As such, we wanted to provide you with information about the incident, and let you know that we continue to take significant measures to protect your personal information.

What Happened?

On October 11, 2024, Sundance became aware of unauthorized access to our network environment.

What Are We Doing?

Upon learning of this issue, we immediately launched an investigation and contained and secured the network. As part of the investigation, we have been working very closely with third-party cybersecurity professionals experienced in handling these types of incidents. After a thorough forensic investigation, we determined on December 16, 2024, that on or about October 11, 2024, certain files containing your personal information may have been accessed and/or acquired by the unauthorized party.

What Information Was Involved?

The data involved contained some of your personal information, including potentially your [redacted]

What Can You Do?

To date, we are not aware of any reports of identity fraud or identity theft as a direct result of this incident. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. To protect you from the potential misuse of your information, we are offering a complimentary identity protection service. These services provide you with alerts when changes occur to your credit file for [redacted] months from the date of enrollment. For more information on identity theft prevention and the credit-monitoring product being offered to you, including instructions on how to activate your complimentary identity protection service, please see the additional information provided below in this letter in the section labeled "Other Important Information."

This letter also provides precautionary measures you can take to protect your personal information, including placing a Fraud Alert and/or Security Freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

For More Information

Sundance values your privacy and deeply regrets that this incident has occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information and will continue to do so in light of this incident.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have established to respond to questions surrounding the incident at [redacted]. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to best protect against the misuse of your information. The response line is available Monday through Friday, [redacted]. Eastern Time, excluding holidays.

Sincerely,

Sundance Holdings Group, LLC
3865 W 2400 S
Salt Lake City, UT 84120

- OTHER IMPORTANT INFORMATION -

1. Enrolling in Complimentary [redacted] month Credit Monitoring.

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted] In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

2. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

3. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

4. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Protecting Your Health Information.

As a general matter the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits" statement which you receive from your health insurance company. Follow up with your insurance company or the care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential disclosure (noted above) to current date.

- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or care provider for any items you do not recognize.

6. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, https://www.marylandattorneygeneral.gov/, Telephone: 888-743-0023.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.