



Laura K Funk
2100 Ross Ave, Suite 2000
Dallas, TX 75201
Laura.Funk@lewisbrisbois.com
Direct: 972.942.5696

April 7, 2022

File No. 34181.927

VIA ELECTRONIC MAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: Idtheft@oag.state.md.us

Re: Notification of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Southland Holdings LLC (“Southland”) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On September 21, 2021, Southland discovered potential unauthorized access to its environment. Upon discovery, Southland took immediate steps to secure its systems prior to restoration. In addition, Southland retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident.

Based on the findings from the investigation, Southland reviewed the affected systems to determine whether personal information was impacted as a result of the incident. Once it was confirmed that data containing personal information was potentially accessed in connection with the incident, a thorough review of the data was undertaken to identify the individuals to whom the information pertained. On February 11, 2022, Southland identified the individuals whose information was potentially affected and diligently worked to obtain up-to-date address information in anticipation of notification.

2. Type of Information and Number of Maryland Residents Involved

The incident involved personal information for approximately two hundred and twenty-two (222) Maryland residents. The information involved may include name, address, Social Security number, and driver's license or state identification number.

The affected individuals will receive a letter notifying them of the incident, offering complimentary identity monitoring services, and providing additional steps they can take to protect their personal information. The identity monitoring services include credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. The notification letters will be sent via U.S. First-Class Mail on April 8, 2022.

3. Measures Taken in Response to the Incident

In response to the incident, Southland implemented additional measures to reduce the risk of a similar incident occurring in the future. As discussed above, Southland is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter. Additionally, Southland has reported the incident to the Federal Bureau of Investigation.

4. Contact Information

Southland is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact me at Laura.Funk@lewisbrisbois.com or 972.942.5696.

Sincerely,



Laura K. Funk of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

LKF/rlw
Encl.: Sample Notification Letter



P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:

1-833-774-2186

Or Visit:

<https://response.idx.us/SouthlandEnrollment>

Enrollment Code: <<Enrollment>>

<<First Name>> <<Last Name>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

April 8, 2022

Notice of <<Header>>

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident experienced by Southland Holdings LLC ("Southland") that may have involved your personal information. Please read carefully, as this letter contains background information about the incident, the type of information involved, and steps you can take to protect your personal information.

What Happened: On September 21, 2021, Southland discovered potential unauthorized access to our environment. Upon discovery, we took immediate steps to secure our systems prior to restoration. In addition, we retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident. Based on the findings from the investigation, we reviewed the affected systems to determine whether personal information was impacted as a result of the incident. Once it was confirmed that data containing personal information was potentially accessed as a result of the incident, an in-depth and thorough review of the data was undertaken to identify the individuals to whom the information pertained. On February 11, 2022, we determined that the affected systems contained some of your personal information.

What Information Was Involved: The information involved may have included your name, address, Social Security number, and driver's license or state identification number.

What We Are Doing: As soon as we learned of the incident, we immediately began containment, mitigation, and restoration efforts. We also launched an investigation and engaged outside cybersecurity experts to assist us in determining what happened. As part of the response processes, we implemented additional security measures to further harden our digital environment in an effort to prevent a similar event from occurring in the future. In addition, we reported the incident to the Federal Bureau of Investigation and are committed to providing the FBI and law enforcement whatever assistance is needed.

Furthermore, even though there is no evidence of misuse of information involved in this incident, we are providing you with information about steps that you can take to help protect your personal information. Additionally, as an added precaution, we are offering you <<12/24 Months>> of identity theft protection services through IDX, a data breach and recovery services expert. These identity protection services include: <<12/24 Months>> of credit monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-774-2186 or going to <https://response.idx.us/SouthlandEnrollment> and using the Enrollment Code provided above. Representatives are available between 8:00am and 8:00pm Central Time from Monday to Friday.

Please note that the deadline to enroll is July 8, 2022. In addition, you can review the resources provided on the following pages for additional steps to protect your personal information.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the credit and identity monitoring services, please call 1-833-774-2186 or go to [https://response.idx.us/Southland Enrollment](https://response.idx.us/SouthlandEnrollment) between 8:00am and 8:00pm Central Time.

The security of your information is a top priority for Southland, and we are committed to safeguarding your data and privacy. Please accept our sincere apologies and know we deeply regret any concern or inconvenience this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "F. Renda", with a stylized flourish at the end.

Frank Renda
Chief Executive Officer
Southland Holdings LLC

Steps You Can Take to Protect Your Personal Information

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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

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 one year. 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: You have the right to put a security freeze on your credit file for up to one year at no cost. This 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

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

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete

inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.