



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

August 17, 2021

File No. 44905.28

CONFIDENTIAL - INTENDED FOR ADDRESSEE(S) ONLY

VIA EMAIL

New Hampshire Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

Re: Notification of Potential Data Security Incident

Dear New Hampshire Office of the Attorney General:

Lewis Brisbois Bisgaard & Smith LLP represents BackNine Insurance and Financial Services, Inc. (“BackNine”) in connection with its recent discovery of misconfigured code that caused certain insurance and annuity applications to be uploaded to one of its publicly accessible cloud storage containers. The purpose of this letter is to notify you of this discovery on behalf of BackNine in accordance with N.H. Rev. Stat. §§ 359-C:19 - C:21.

1. Background

BackNine is an insurance broker and a financial services firm headquartered in Westlake Village, California. BackNine sells life, long term care, and disability insurance as well as annuities.

On July 12, 2021, BackNine learned of a coding error that caused certain insurance and annuity applications to be uploaded to one of its publicly accessible cloud storage containers. Upon discovering this information, BackNine immediately changed the settings applicable to the relevant cloud storage container so that the cloud storage container at issue was no longer publicly accessible. BackNine also audited all other cloud storage containers to ensure that it was the only one affected and altered the misconfigured code to ensure that insurance and annuity applications would no longer be inadvertently uploaded to a publicly accessible container.

BackNine has no evidence that any potentially impacted information has been misused.

INTENDED FOR ADDRESSEE(S) ONLY
New Hampshire Office of the Attorney General
August 17, 2021
Page 2

2. Type of Information and Number of New Hampshire Residents Involved

On August 13, 2021, BackNine provided notification of this incident to 50 potentially impacted New Hampshire residents. The information potentially involved varies depending on the individual but may have included name, address, phone number, date of birth, Social Security number, driver's license or state identification card number, health-related information, and/or financial status (*e.g.*, assets, liabilities, and income). Sample notification letters are enclosed.

3. Remediation Measures

Upon learning of this incident, BackNine immediately changed the settings of the relevant cloud storage container to ensure that information contained therein was no longer publicly accessible. BackNine also audited all other cloud storage containers to ensure that it was the only one affected and altered the misconfigured code to ensure that insurance and annuity applications would no longer be inadvertently uploaded to a publicly accessible container.

BackNine is dedicated to protecting the sensitive information of its customers. If you have questions or need any additional information, please do not hesitate to contact me at 720.292.2052 or Alyssa.Watzman@lewisbrisbois.com. Jennifer Lee (714.668.5568 | Jennifer.Lee@lewisbrisbois.com) and Vy Nguyen (646.783.0998 | Vy.Nguyen@lewisbrisbois.com) are also available to address any follow up inquiries.

Sincerely,



Alyssa R. Watzman of
LEWIS BRISBOIS BISGAARD & SMITH LLP

ARW:JL

Encl. Sample Consumer Notification Letters
cc: Jennifer Lee, Lewis Brisbois (Jennifer.Lee@lewisbrisbois.com)
Vy Nguyen, Lewis Brisbois (Vy.Nguyen@lewisbrisbois.com)



<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Visit:
<https://response.idx.us/backnine>
Or Call:
(833) 909-3934
Enrollment Code: <<XXXXXXXXXX>>

August 13, 2021

Re: Notice of Data Breach

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

I am writing to inform you of a recent data security issue discovered by BackNine Insurance and Financial Services, Inc. (“BackNine”) that may have impacted your personal information. Please read carefully as this letter contains background information about the issue, the type of information potentially involved, and steps that you can take to help protect your personal information, including enrolling in the complimentary identity protection services offered below.

What Happened. BackNine is an insurance broker and financial services firm located in Westlake Village, California. BackNine sells life, long term care, and disability insurance as well as annuities.

On July 12, 2021, BackNine learned of a coding error that caused certain insurance and annuity applications to be uploaded to a publicly accessible folder on its cloud storage system. Upon discovery, BackNine immediately secured the folder so that it was no longer publicly accessible. BackNine also audited the cloud storage system to confirm that the folder at issue was the only one affected and altered the misconfigured code to ensure that future applications would be uploaded to and stored in the intended, non-publicly accessible folders.

In addition, BackNine—with the assistance of outside data privacy and cybersecurity experts—conducted an investigation and worked to identify the individuals whose personal information was stored in the impacted cloud storage folder and the categories of information potentially involved for each such individual. On July 26, 2021, we determined that the impacted folder contained some of your personal information. We then worked diligently to identify current address information required to provide notification of this incident.

We have no reason to believe that your information was accessed, acquired, or misused. Nevertheless, we are notifying you of this issue out of an abundance of caution so that you may take appropriate steps to help protect your personal information.

What Information Was Involved. The impacted cloud storage folder contained the following information provided by you to BackNine in connection with your <<Role/Policy Type>>: <<data elements>>.

What We Are Doing. As soon as we learned of the issue, we took the measures referenced above. We are also implementing additional security measures to protect the information on our systems and to minimize the likelihood of a similar situation occurring in the future. Furthermore, we are providing you information about steps you can take to help protect your personal information and offering free identity protection services for <<12 or 24 months>> through IDX.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We also strongly encourage you to enroll in the complimentary identity protection services. These services include credit monitoring,* CyberScan monitoring, a \$1,000,000 identify theft insurance reimbursement policy, and fully managed identity recovery services. To enroll, please go to <https://response.idx.us/backnine> or call **(833) 909-3934** and use the Enrollment Code provided at the top of this letter. The deadline to enroll is **November 13, 2021**.

For More Information. If you have any questions regarding the incident or would like assistance with enrolling in the identity protection services offered to you through IDX, please call **(833) 909-3934** between Monday through Friday from 6 a.m. to 6 p.m. Pacific Time.

*To receive credit monitoring services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

BackNine is committed to protecting the security and privacy of its customers. We regret any worry or inconvenience that this may cause you.

Sincerely,

Reid Tattersall

Reid Tattersall, Vice President
BackNine Insurance and Financial Services, Inc.

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>.



<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Visit:
<https://response.idx.us/backnine>
Or Call:
(833) 909-3934
Enrollment Code: <<XXXXXXXXXX>>

August 13, 2021

Re: Notice of Data Breach

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

I am writing to inform you of a recent data security issue discovered by BackNine Insurance and Financial Services, Inc. (“BackNine”) that may have impacted your personal information. Please read carefully as this letter contains background information about the issue, the type of information potentially involved, and steps that you can take to help protect your personal information, including enrolling in the complimentary identity protection services offered below.

What Happened. BackNine is an insurance broker and financial services firm located in Westlake Village, California. BackNine sells life, long term care, and disability insurance as well as annuities.

On July 12, 2021, BackNine learned of a coding error that caused certain insurance and annuity applications to be uploaded to a publicly accessible folder on its cloud storage system. Upon discovery, BackNine immediately secured the folder so that it was no longer publicly accessible. BackNine also audited the cloud storage system to confirm that the folder at issue was the only one affected and altered the misconfigured code to ensure that future applications would be uploaded to and stored in the intended, non-publicly accessible folders.

In addition, BackNine—with the assistance of outside data privacy and cybersecurity experts—conducted an investigation and worked to identify the individuals whose personal information was stored in the impacted cloud storage folder and the categories of information potentially involved for each such individual. On July 26, 2021, we determined that the impacted folder contained some of your personal information. We then worked diligently to identify current address information required to provide notification of this incident.

We have no reason to believe that your information was accessed, acquired, or misused. Nevertheless, we are notifying you of this issue out of an abundance of caution so that you may take appropriate steps to help protect your personal information.

What Information Was Involved. The impacted cloud storage folder contained the following information provided by the applicant to BackNine while designating you as a <<Role/Policy Type>>: <<data elements>>.

What We Are Doing. As soon as we learned of the issue, we took the measures referenced above. We are also implementing additional security measures to protect the information on our systems and to minimize the likelihood of a similar situation occurring in the future. Furthermore, we are providing you information about steps you can take to help protect your personal information and offering free identity protection services for <<12 or 24 months>> through IDX.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We also strongly encourage you to enroll in the complimentary identity protection services. These services include credit monitoring,* CyberScan monitoring, a \$1,000,000 identify theft insurance reimbursement policy, and fully managed identity recovery services. To enroll, please go to <https://response.idx.us/backnine> or call **(833) 909-3934** and use the Enrollment Code provided at the top of this letter. The deadline to enroll is **November 13, 2021**.

For More Information. If you have any questions regarding the incident or would like assistance with enrolling in the identity protection services offered to you through IDX, please call **(833) 909-3934** between Monday through Friday from 6 a.m. to 6 p.m. Pacific Time.

*To receive credit monitoring services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

BackNine is committed to protecting the security and privacy of its customers. We regret any worry or inconvenience that this may cause you.

Sincerely,

Reid Tattersall

Reid Tattersall, Vice President
BackNine Insurance and Financial Services, Inc.

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>.



<<Return Address>>
<<City>>, <<State>> <<Zip>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Visit:
<https://response.idx.us/backnine>
Or Call:
(833) 909-3934
Enrollment Code: <<XXXXXXXXXX>>

August 13, 2021

Re: Notice of Data Breach

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

I am writing to inform you of a recent data security issue discovered by BackNine Insurance and Financial Services, Inc. (“BackNine”) that may have impacted your personal information (“PI”) and protected health information (“PHI”). Please read carefully as this letter contains background information about the issue, the type of information potentially involved, and steps that you can take to help protect your information, including enrolling in the complimentary identity protection services offered below.

What Happened. BackNine is an insurance broker and financial services firm located in Westlake Village, California. BackNine sells life, long term care, and disability insurance as well as annuities.

On July 12, 2021, BackNine learned of a coding error that caused certain insurance and annuity applications to be uploaded to a publicly accessible folder on its cloud storage system. Upon discovery, BackNine immediately secured the folder so that it was no longer publicly accessible. BackNine also audited the cloud storage system to confirm that the folder at issue was the only one affected and altered the misconfigured code to ensure that future applications would be uploaded to and stored in the intended, non-publicly accessible folders.

In addition, BackNine—with the assistance of outside data privacy and cybersecurity experts—conducted an investigation and worked to identify the individuals whose information was stored in the impacted cloud storage folder and the categories of information potentially involved for each such individual. On July 26, 2021, we determined that the impacted folder contained some of your PI and PHI. We then worked diligently to identify current address information required to provide notification of this incident.

We have no reason to believe that your information was accessed, acquired, or misused. Nevertheless, we are notifying you of this issue out of an abundance of caution so that you may take appropriate steps to help protect your PI and PHI.

What Information Was Involved. The impacted cloud storage folder contained the following information provided by you to BackNine in connection with your <<Role/Policy Type>>: <<data elements>>.

What We Are Doing. As soon as we learned of the issue, we took the measures referenced above. We are also implementing additional security measures to protect the information on our systems and to minimize the likelihood of a similar situation occurring in the future. Furthermore, we are providing you information about steps you can take to help protect your PI/PHI and offering free identity protection services for <<12 or 24 months>> through IDX.

What You Can Do. You can follow the recommendations included with this letter to protect your information. We also strongly encourage you to enroll in the complimentary identity protection services. These services include credit monitoring,* CyberScan monitoring, a \$1,000,000 identify theft insurance reimbursement policy, and fully managed identity recovery services. To enroll, please go to <https://response.idx.us/backnine> or call **(833) 909-3934** and use the Enrollment Code provided at the top of this letter. The deadline to enroll is **November 13, 2021**.

For More Information. If you have any questions regarding the incident or would like assistance with enrolling in the identity protection services offered to you through IDX, please call **(833) 909-3934** between Monday through Friday from 6 a.m. to 6 p.m. Pacific Time.

*To receive credit monitoring services, you must be over the age of 18, have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

BackNine is committed to protecting the security and privacy of its customers. We regret any worry or inconvenience that this may cause you.

Sincerely,

Reid Tattersall

Reid Tattersall, Vice President
BackNine Insurance and Financial Services, Inc.

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>.