



Michael Christopher, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East, Suite 1100
Los Angeles, CA 90067
mchristopher@constangy.com
Direct: 310.912.6183
Mobile: 949-322-8874

July 19, 2024

Via Email

Attorney General Anthony Brown
Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete, LLP represents Congoleum Acquisition LLC ("Congoleum"), a company based in New Jersey, 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.

1. What Happened

On June 30, 2024, Congoleum discovered unusual activity in its digital environment. Upon discovering this activity, it immediately took steps to secure the network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, Congoleum learned that an unauthorized actor acquired certain files and data stored within its systems. Upon learning this, Congoleum launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. Following the completion of this comprehensive review, Congoleum confirmed on July 11, 2024, that certain individuals' personal information may have been involved in the incident. Since that time, Congoleum has been working to gather contact information for individuals and prepare notification to all affected individuals of this incident. That review continues at this time.

2. Number of Maryland Residents Notified and Type of Information

On July 19, 2024, and in coordination with its relevant clients, Congoleum began notifying fifty-one (1) Maryland residents of this data security incident via U.S. First-Class Mail. The data sets affected by this incident included individuals' names, Social Security numbers, or driver's license numbers. A sample copy of the notification letter sent to potentially impacted individuals known at this time is included with this correspondence.

3. Steps Taken Relating to the Incident

Congoleum has implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, Congoleum has offered notified individuals 12 months of complimentary services through IDX,

July 19, 2024

Page 2

which includes credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

4. Contact Information

Congoleum remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please contact me.

Very truly yours,

A handwritten signature in blue ink, appearing to read "MC" or similar initials, followed by a stylized flourish.

Michael Christopher
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter



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

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>> or <<IMB>>

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

July 19, 2024

Notice of Data Security Incident

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

Congoleum Acquisition, LLC (“Congoleum”) is writing to inform you of a recent data security incident that may have involved your personal information. Congoleum takes the privacy and security of all information within its possession very seriously. We are writing to notify you about the incident, provide you with information about steps you can take to help protect your information, and offer you the opportunity to enroll in complimentary identity protection services that Congoleum is making available to you.

What Happened? On June 30, 2024, we discovered unusual activity in our digital environment. Upon discovering this activity, we immediately took steps to secure the network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, we learned that an unauthorized actor acquired certain files and data stored within our systems. Upon learning this, we launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. Following the completion of this comprehensive review, we confirmed on July 11, 2024, that your personal information may have been involved in the incident. Since that time, we have been working to gather contact information for individuals and prepare notification to all affected individuals of this incident.

What Information Was Involved? Following our review of the contents of the impacted data, on July 11, 2024, we determined that your name, Social Security numbers or driver’s license numbers were included. We emphasize that we have no evidence of any actual or attempted misuse of this information.

What Are We Doing? As soon as we discovered this incident, we took measures to further secure the network and enlisted outside cybersecurity experts to conduct a forensic investigation. We have also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. In addition, we are notifying you of this event and providing resources you can utilize to help protect your information.

As a precaution, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised

What Can You Do? We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. Please note the deadline to enroll is October 19, 2024. We also recommend that you review the guidance included with this letter about how to protect your information.

For More Information: If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-939-4170 and supply the call specialist with your unique code listed above.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Congoleum Acquisition, LLC
3500 Quakerbridge Rd.
Trenton, NJ 08619

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 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
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
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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>
riag.ri.gov
1-401-274-4400

New Jersey State Police

Cyber Crime Unit
(609) 584-5051 ext. 5664
<https://www.nj.gov/njsp/division/investigations/cyber-crimes.html>

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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.



Michael Christopher, Partner
Cybersecurity & Data Privacy Team
2029 Century Park East, Suite 1100
Los Angeles, CA 90067
mchristopher@constangy.com
Direct: 310.912.6183
Mobile: 949-322-8874

August 7, 2024

VIA EMAIL

Attorney General Anthony Brown
Office of the Attorney General
ATTN: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notice of Data Security Incident

To Whom It May Concern:

This letter is to provide an update regarding the recent data security incident experienced by Congoleum Acquisition LLC ("Congoleum") described in our previous correspondence dated July 19, 2024.

On August 7, 2024, Congoleum mailed notification letters to an additional ninety-one (91) Maryland residents whose information may have been impacted by this incident. The affected personal information includes individuals' names and Social Security numbers. The letter includes information notifying them of the incident, offering complimentary identity protection services, and providing additional steps they can take to protect their personal information. A copy of the sample notification letter is enclosed.

Congoleum remains dedicated to protecting the information in its possession. If you have any questions or need additional information, please contact me.

Very truly yours,

A handwritten signature in blue ink, appearing to read "MC", is written over a faint, light blue rectangular background.

Michael Christopher
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Enclosure: Sample Notification Letter



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

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>> or <<IMB>>

Enrollment Code: <<XXXXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

August 7, 2024

Notice of <<Variable Data>>

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

Congoleum Acquisition, LLC (“Congoleum”) is writing to inform you of a recent data security incident that may have involved your personal information. Congoleum takes the privacy and security of all information within its possession very seriously. We are writing to notify you about the incident, provide you with information about steps you can take to help protect your information, and offer you the opportunity to enroll in complimentary identity protection services that Congoleum is making available to you.

What Happened? On June 30, 2024, we discovered unusual activity in our digital environment. Upon discovering this activity, we immediately took steps to secure the network and launched an investigation, aided by independent cybersecurity experts, to determine what happened and whether sensitive information may have been affected. As a result of the investigation, we learned that an unauthorized actor acquired certain files and data stored within our systems. Upon learning this, we launched a comprehensive review of all potentially affected information to identify any personal information that could have possibly been acquired. Following the completion of this comprehensive review, we confirmed on July 11, 2024, that your personal information may have been involved in the incident. Since that time, we have been working to gather contact information for individuals and prepare notification to all affected individuals of this incident.

What Information Was Involved? Following our review of the contents of the impacted data, on July 11, 2024, we determined that your name and Social Security number was included. We emphasize that we have no evidence of any actual or attempted misuse of this information.

What Are We Doing? As soon as we discovered this incident, we took measures to further secure the network and enlisted outside cybersecurity experts to conduct a forensic investigation. We have also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. In addition, we are notifying you of this event and providing resources you can utilize to help protect your information.

As a precaution, we are offering identity theft protection services through IDX, A ZeroFox Company, the data breach and recovery services expert. IDX identity protection services include: <<12 months/24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised

What Can You Do? We encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-800-939-4170, going to <https://app.idx.us/account-creation/protect>, or scanning the QR image and using the Enrollment Code provided above. Please note the deadline to enroll is November 7, 2024. We also recommend that you review the guidance included with this letter about how to protect your information.

For More Information: If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 9:00 am to 9:00 pm Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-939-4170 and supply the call specialist with your unique code listed above.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Congoleum Acquisition, 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 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-800-831-5614
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
1-877-438-4338

Maryland Attorney General

St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

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>
riag.ri.gov
1-401-274-4400

New Jersey State Police

Cyber Crime Unit
(609) 584-5051 ext. 5664
<https://www.nj.gov/njsp/division/investigations/cyber-crimes.html>

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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>.

A total of 1,661 individuals are being notified of this incident.