



20568

[DAY], May [] , 2021

NOTICE OF DATA BREACH

Dear [Insert name]:

We are contacting you about a data breach that has occurred at Congo, LLC.

What happened?	Congo recently discovered that company emails were accessed due to the unauthorized use of a compromised Office 365 administrative account. The exact date of the initial breach is unknown but may have occurred sometime in March 2021. Immediately following this discovery, we took action to determine the scope of the breach, to restore the reasonable integrity of the data system and to prevent any further unauthorized access. We do not know what, if any, information contained in the company emails was stolen or misused; however, out of an abundance of caution, we contact you because it is possible that your personally identifying information was compromised.
What Information Was Involved?	We do not have specific knowledge that your personal information was accessed; however, based on the nature of the breach, it is possible that any personal information sent by you or contained in company emails may have been exposed, including your name, social security number, driver's license number, bank account information, and any other information provided to Congo.
What We Are Doing	<p>After the breach was discovered, we immediately hired a forensic IT team to identify the source and the scope of the breach and to take actions to stop the breach and safeguard our systems. In addition, we implemented additional access controls and security policies to further ensure the security of our data.</p> <p>Moreover, we are offering you, free of charge, two years of credit monitoring. If you would like to exercise this offer, please send an email to ITsecurity@congobrands.com with the subject line "Credit Monitoring."</p>
What You Can Do	<p>The Federal Trade Commission (FTC) recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. As soon as one credit bureau confirms your fraud alert, the others are automatically notified to place fraud alerts on your account. The initial fraud alert stays on your credit report for one year, and you can renew it again.</p> <ol style="list-style-type: none"> 1. Equifax: http://www.equifax.com/personal/credit-report-services/ or 1-800-685-1111. 2. Experian: http://www.experian.com/help/ or 1-888-397-3742.



[DAY], May , 2021

	<p>3. TransUnion: http://www.transunion.com/credit-help or 1-888-909-8872</p> <p>Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries that you do not recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's site at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.</p> <p>You may also want to consider placing a free credit freeze. A credit freeze means potential creditors cannot get your credit report, which makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.</p>
For More Information	<p>If you have additional questions about this Notice, please email ITsecurity@congobrands.com.</p> <p>Congo, LLC 7201 Intermodal Drive STE A Louisville, Kentucky 40258</p>



[DAY], May [DAY], 2021

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review 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 should also 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 (the "FTC").

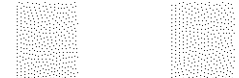
Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to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

Equifax	Experian	TransUnion	Free Annual Report
P.O. Box 105851	P.O. Box	P.O. Box	P.O. Box
Atlanta, GA 30348	9532 Allen,	1000	105281
1-800-525-6285	TX 75013	Chester, PA	Atlanta, GA
www.equifax.com	1-888-397-	190161-800-	303481-877-
	3742	916-8800	322-8228
	www.experian.com	www.transunion.com	www.annualcreditreport.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 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: Under U.S. law, 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 your Attorney General. Further recommended privacy protection steps are outlined in the Breach Help – Consumer Tips from the California Attorney General, and can be found at: <https://oag.ca.gov/sites/all/files/agweb/pdfs/privacy/cis-17-breach-help.pdf>.



[DAY], May _____, 2021

**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

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

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

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.