



Linda Z. Spencer
Chief Privacy Officer

One Coca-Cola Plaza, NW
Atlanta, GA 30313
T 404-676-4711
F 404-598-4711
lindaspencer@coca-cola.com

January 19, 2018

Via FedEx

Attorney General Gordon J. MacDonald
NH Department of Justice
33 Capitol Street
Concord, NH 03301

STATE OF NH
DEPT OF JUSTICE
2018 JAN 22 PM 3:32

Dear Attorney General MacDonald:

We are writing to notify you of a data security incident involving certain employees of The Coca-Cola Company ("Coca-Cola"), in accordance with N.H. Rev. Stat. § 359-C:20. Coca-Cola is a Delaware-incorporated company with its headquarters in Atlanta, Georgia.

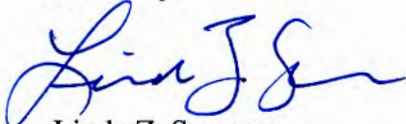
From approximately July to November 2017, certain employees of Coca-Cola received phishing emails in which they were asked to provide their network log-in credentials. In late September, we identified an instance of unauthorized access into a Coca-Cola employee's email account that resulted from this phishing incident. After we discovered this incident, we promptly took steps to determine whether any personally identifiable information ("PII") may have been accessed, and to implement enhanced security protocols to prevent any further unauthorized access. Beginning in late November, our investigation identified documents containing personal information for approximately 2,181 individuals that may have been compromised during the phishing incident.

Of the affected individuals, 1 is a resident of the state of New Hampshire. At this time, it appears that only names, employee ID numbers, and social security numbers may have been compromised.

Coca-Cola will be mailing notifications to affected individual residents of New Hampshire on January 22, 2018. A sample copy of the notification letter for those individuals is included as an attachment to this letter. All affected individuals will be offered one year of free identity monitoring services through a third-party provider.

Coca-Cola is continuing to investigate whether any other individuals' PII may have been accessed during this incident, and will notify any other affected individuals as required as our investigation continues.

Sincerely,

A handwritten signature in blue ink, appearing to read "Linda Z. Spencer". The signature is fluid and cursive, with the first name "Linda" being the most prominent.

Linda Z. Spencer

Enclosure



The Coca-Cola Company
One Coca-Cola Plaza
Atlanta, GA 30313

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <NameSuffix>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

On behalf of The Coca-Cola Company ("Coca-Cola"), I am writing to tell you about a data security incident that may have exposed some of your personal information. We take the protection and proper use of your information very seriously and we deeply regret that this happened.

What happened?

In late September, we identified unauthorized access to certain Coca-Cola email accounts that resulted from a phishing incident. After we discovered this incident, we promptly took steps to resolve it and began to investigate and address it. Based on our investigation, we believe that from approximately July to November 2017, certain employees of Coca-Cola were targeted by a phishing scam. Beginning in late November, our investigation identified documents containing certain personal information that may have been compromised during the phishing incident. In addition to remediation measures, our investigation is continuing to ensure we understand the full scope and potential impact of the situation.

We have notified, or are in the process of notifying, the relevant authorities.

What information was involved?

We are notifying you because your personal information appeared in the documents that may have been accessed during the phishing incident. As a result of the data breach, unauthorized individuals may have gained access to certain personally identifiable information ("PII") about you, including your name, your employee ID number, login credentials (e.g., user name or email address and security code, access code, PIN, or password), your government identification number(s) (e.g., Social Security number, Tax Identification Number, Passport number, and/or other government identification numbers), and/or your credit and/or debit card information or financial account information.

What we are doing.

After learning of the attack, we have taken steps to improve our security environment. We changed the impacted users' passwords and provided notices to all of the individuals who clicked the link in the phishing e-mail. We are also continuing to conduct a forensic review of e-mail inboxes for individuals whose credentials were compromised and who were likely to have PII about other Coca-Cola employees. Coca-Cola's IT department is also continuing to work with our software vendor to prevent more sophisticated attempts to access Coca-Cola accounts using the credentials that were previously obtained.

To help alleviate concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring for one year at no cost to you. Kroll has extensive experience in risk mitigation and response, and in helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

It is important that you remain vigilant against possible identity theft by regularly reviewing your account statements and credit reports.

Visit my.idmonitoringservice.com to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-833-214-8739. Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call 1-833-214-8739, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,



Linda Z. Spencer
Chief Privacy Officer
The Coca-Cola Company

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies is:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit www.annualcreditreport.com or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. The credit reporting agencies may charge a fee to place a freeze, temporarily lift it or permanently remove it. The fee is waived if you are a victim of identity theft and have submitted a valid investigative or law enforcement report or complaint relating to the identity theft incident to the credit reporting agencies. (You must review your state's requirement(s) and/or credit bureau requirement(s) for the specific document(s) to be submitted.)

For Massachusetts residents: The fee for each placement of a freeze, temporary lift of a freeze, or removal of a freeze is \$5.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and 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.