AIREFCO
"A DIFFERENCE YOU CAN FEEL"

Tualatin Office | 18755 SW Teton Ave • Tualatin, OR 97062 • 503-692-3210 • 503-691-2392 Fax
Fife Office | 2101 Frank Albert Rd E • Fife, WA 98424 • 253-886-5350 • 253-886-5353 Fax
Spokane Office | 2600 E. Ferry Ave • Spokane, WA 99202 • 509-536-1811 • 509-536-4009 Fax

December 6, 2023

[redacted], MT 59101

NOTICE OF DATA BREACH

Dear [redacted]:

We are writing to you because Airefco, Inc. ("Airefco") recently identified a data security incident that may have disclosed some of your personal information. Although there is no indication that specific documents containing your personal information were actually accessed or disclosed during the incident, after the completion of our comprehensive investigation and review of the circumstances, we are contacting you directly to make you aware of the types of information that may have been potentially disclosed so that you can remain vigilant and undertake any security measures you may deem appropriate.

What Happened

On August 17, 2023, Airefco determined that an email account of one of its employees had been compromised as a result of an unauthorized actor gaining access to the email account. An investigation was launched immediately that included a comprehensive review of available information regarding activity in the email account, as well as a thorough review of all potentially affected Airefco systems to ensure that all those systems were secure. Along with its investigation by the internal Information Technology team, Airefco also retained an independent forensic investigation team to review available account activity information and the potentially affected Airefco systems.

The investigation revealed that the unauthorized access, which occurred between June 9, 2023 and July 6, 2023, had been terminated and blocked as of July 6, 2023 so that the unauthorized actor could not access any information or documents after that date. The investigation also revealed that the unauthorized actor appeared to be focused on attempting to obtain business account invoicing and wire transfer information, possibly in an attempt to further a fraudulent wire transfer scheme.

What Information Was Involved

The forensic investigation and analysis by the internal Information Technology team and the independent forensic team did not identify any information that indicates specific documents containing your personal information were actually accessed by or disclosed to the unauthorized actor.

However, after completing the comprehensive investigation and review of the circumstances and available information, we have determined that information and documents in the single email account at issue contained the following categories of your personal information that may have been potentially exposed: Social Security number.

What We Are Doing

As part of our ongoing efforts to help prevent something like this from happening in the future, Airefco has implemented several changes to protect data from any subsequent incidents. We are working to identify vulnerabilities in our systems and implement appropriate remedial action, as well as enhance our employee training protocols. Additionally, we are accelerating our efforts to further harden our environment through various enhancements and other security measures, and will utilize the information revealed in the analysis of this incident to further strengthen the security of our network, systems and information.

What You Can Do, and For More Information

Although there is no information to confirm that any of your personal information has been accessed or obtained by the unauthorized actor, as a best practice, we recommend you remain vigilant, including carefully reviewing account statements. Out of an abundance of caution, you may wish to change your username, password, and/or security questions relevant to the information listed above as being potentially compromised.

Please also 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, details on how to place a fraud alert or a security freeze on your credit file, and other identity theft prevention and mitigation tools and services. You have a right to obtain a police report if you are the victim of identity theft.

Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 12 months. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, and $1 Million Identity Fraud Loss Reimbursement. More information describing these services is included with this letter.

- Visit **https://krollmonitoring.com/redeem** to activate and take advantage of your identity monitoring services.
- You *have until* ***January 6, 2024*** *to activate your identity monitoring services.*
- **Activation Code: [redacted]MBRR**
- **Verification ID: SF[redacted]**

Additional information about Kroll and your identity monitoring services can be found at **https://www.info.krollmonitoring.com**. We recommend that you activate your complimentary identity monitoring services.

Finally, in the event there is any suspicious activity in any of your accounts or you suspect you are the victim of identity theft, you should promptly notify the financial institution where the account is maintained and report the activity to the proper law enforcement authorities.

Your trust in Airefco is of paramount importance to us, and we deeply regret that this incident occurred.

If you have questions, please contact Airefco's attorney in connection with this matter, John Wolak, Esq. of Gibbons P.C. at 973-596-4725 Monday through Friday from 9:00 a.m. to 5:00 p.m. Eastern Time.

Sincerely,

Steven R. Johnson, District Vice President
Airefco, Inc.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

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 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. 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 Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

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 use an online process, an automated telephone line, or submit 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 5 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, and display your name, current mailing address, and the date of issue.

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 minimize the risks of 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.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

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.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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 will be able to help you determine if it is 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 will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will 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.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

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.