McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic Paluzzi
Direct Dial: 248-220-1356
E-mail: dpaluzzi@mcdonaldhopkins.com

August 28, 2020

VIA EMAIL (SecurityBreach@atg.wa.gov)

Office of the Attorney General
1125 Washington St SE
PO Box 40100
Olympia, WA 98504

Re: AliMed, Inc. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents AliMed, Inc. I am writing to provide notification of an incident at AliMed that may affect the security of payment card information of approximately six hundred and seventy-two (672) Washington residents. AliMed's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, AliMed does not waive any rights or defenses regarding the applicability of Washington law or personal jurisdiction.

AliMed recently discovered that a malicious party had gained access to one of their servers and may have acquired payment card data used in connection with certain transactions made with AliMed. Upon learning this, AliMed engaged external forensic investigators and data privacy professionals and commenced a prompt and thorough investigation into the incident. As a result of this investigation, it was determined on July 27, 2020 that the payment card information potentially accessed and/or acquired related to certain transactions made with AliMed between June 1, 2019 and June 17, 2020.

To date, AliMed has no evidence that any of the information has been misused. Nevertheless, out of an abundance of caution, AliMed wanted to inform you (and the affected residents) of the incident and to explain the steps it is taking to help safeguard the affected residents against identity fraud. AliMed is providing the affected residents with written notification of this incident commencing on or about August 27, 2020 in substantially the same form as the letter attached hereto. This notice advises the residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. AliMed is also providing the contact information for the consumer reporting agencies, and the Federal Trade Commission.

At AliMed, protecting the privacy of personal information is a top priority. AliMed is committed to maintaining the privacy of personal information in its possession and has taken

many precautions to safeguard it. AliMed continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

Should you have any questions concerning this notification, please contact me at 248-220-1356 or dpaluzzi@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

Dominic Paluzzi

Encl.

AliMed®
Helping people...help people™

[redacted]

August 26, 2020

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted],

We are writing to make you aware of a recent data security incident involving potential unauthorized access to some of our customers' payment card data. The privacy and security of your personal information is of utmost importance to AliMed, Inc. ("AliMed") and we are routinely evaluating and enhancing our security and payment systems to ensure your information is secure.

What Happened?

We recently discovered that a malicious party had gained access to one of our servers and may have acquired payment card data used in connection with certain transactions made with AliMed. We engaged external forensic investigators and data privacy professionals and commenced a prompt and thorough investigation into the incident. As a result of this investigation, we determined that the payment card information potentially accessed and/or acquired related to certain transactions made with AliMed between June 1, 2019 and June 17, 2020.

What Information Was Involved?

The information that may have been accessed and/or acquired in this incident included customer name, credit or debit card number(s), card expiration date(s) and CVV code(s) (3 or 4 digit code on the front or back of the card). We discovered on July 27, 2020 that you placed an order with AliMed during the window of compromise with your card ending in [redacted].

What We Are Doing

Because we value our relationship with you, we wanted to make you aware of the incident. We also wanted to let you know what we are doing to further secure your information, and suggest steps you can take. Since learning of the incident, we have implemented enhanced security safeguards to help protect against similar intrusions. We are also conducting ongoing monitoring of our network to ensure that it is secure and clear of any malicious activity and actors.

What You Can Do

Enclosed you will find precautionary measures you can take to help protect your personal information. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

As a best practice, you should also call your bank or card issuer if you see any suspicious transactions. The policies of the payment card brands such as Visa, MasterCard, American Express and Discover provide that you are not liable for any unauthorized charges if you report them in a timely manner. You may also ask your bank or card issuer whether a new card should be issued to you.

For More Information

Your trust is a top priority for AliMed, and we deeply regret the inconvenience this may have caused. The privacy and protection of our customers' information is a matter we take seriously.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line to respond to questions at 1-844-480-0275. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time.

Thank you,

AliMed, Inc.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert.

You may place an initial one-year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/
1-800-349-9960	1-888-397-3742	securityfreeze
		1-888-909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.