

February 24, 2025

Colman McCarthy

VIA email to idtheft@oag.state.md.us
Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

2555 Grand Blvd.
Kansas City, MO 64108
dd 816.559.2081
cdmccarthy@shb.com

RE: OneWater Marine Inc. - Security Incident

Dear Sir/Madam:

I am writing on behalf of OneWater Marine Inc. ("OneWater") to notify you of a security incident involving the personal information of five (5) Maryland residents.

On September 3, 2024, OneWater identified suspicious activity related to an employee email account. OneWater promptly engaged Shook, Hardy & Bacon as outside counsel, and Shook, in turn, engaged a digital-forensics firm to assist in the investigation. The investigation subsequently determined that an unauthorized third party gained access to a OneWater Marine employee email account from September 2-3, 2024.

Once it was determined that files were affected, a data-review firm was also engaged to determine what personal information, if any, was in those files. The data review identified the following types of personal information: name and health or medical information. Since then, Shook has been diligently working with OneWater to identify the correct addresses for the affected individuals, which was completed on January 23, 2025, and then assess the corresponding notification obligations.

On February 24, 2025, OneWater started mailing written notice to the affected individuals informing them that an unauthorized third party may have accessed some of their personal information, and we have attached a template of the notification letter.

In addition to providing notice, OneWater has taken a variety of measures to bolster the security of the email account, including password and MFA token reset.

Please contact me if you have any questions or need any additional information regarding this incident.

Sincerely,



Colman McCarthy
Partner



February 24, 2025

VIA U.S. MAIL

<Name>

<Company>

<Address>

<City>, <State> <ZIP>

Dear <Name>,

On behalf of OneWater Marine Inc. and its subsidiaries and affiliates (“OneWater Marine”), I am writing to inform you of an incident involving unauthorized access to some of your information. In September 2024, we detected suspicious activity related to a OneWater Marine employee email account. We promptly began investigating, and have recently determined that some of your personal information was involved in this incident. We are providing this notice to give you information on what happened and what we are doing in response.

WHAT HAPPENED

An unauthorized third party had access to an employee email account between September 2-3, 2024. We engaged cybersecurity experts to assist in the investigation and, once we identified the impacted data, we engaged a data-review firm to review the contents of those files. Since we received the results, we have diligently been working to get accurate contact information for notifying impacted individuals.

WHAT INFORMATION WAS INVOLVED

Based on the investigation, we determined that the unauthorized third party accessed emails and documents in the email account that contained some of your personal information. Impacted data may include your name, health information, and medical information.

WHAT WE ARE DOING

We hired third-party experts to address this situation, perform an investigation into the unauthorized activity, and further secure our systems to protect your information.

WHAT YOU CAN DO

We encourage you to remain vigilant for any signs of unauthorized financial activity. Please also review the next page for other steps you can take to protect yourself against fraud and identity theft.

FOR MORE INFORMATION

Should you have any questions or concerns, you can contact us at 678-541-6300, and we will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

A handwritten signature in blue ink, appearing to read "Josh Richey".

Josh Richey
General Counsel

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – We encourage you to remain vigilant for fraud or identity theft by reviewing your account statements and free credit reports. You can also find additional suggestions at www.identitytheft.gov/Info-Lost-or-Stolen.

- You can confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You can obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling (877) 322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency. The alert lasts for one year, but you can renew it.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which makes it harder for someone to open an account in your name. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. There is no charge for requesting a security freeze. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider (1) notifying your Attorney General, local law enforcement, or the Federal Trade Commission; (2) filing a police report and requesting a copy of that report; and (3) visiting www.IdentityTheft.gov to report the issue and get recovery steps.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Equifax
P.O. Box 740241
Atlanta, GA 30374
(800) 685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013
(888) 397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
(888) 909-8872
www.transunion.com

**Maryland
Attorney General**
200 St. Paul Place, 25th Floor
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, DC 20580
(202) 326-2222
www.ftc.gov

You can also find your Attorney General's contact information at: <https://www.usa.gov/state-attorney-general>.