April 25, 2025

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Submission:

Attorney General Nicholas W. Brown
1125 Washington St SE
PO Box 40100
Olympia, WA 98504
(360) 753-6200
Email: SecurityBreach@atg.wa.gov

Re: Cybersecurity Incident Involving Marine Floats LLC

Dear Attorney General Brown:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Marine Floats LLC ("MF"), a business that designs, builds, and maintains custom waterfront structures, located at 313 East F St., Tacoma, WA 98421, with respect to a recent cybersecurity incident that was first discovered by MF on or around November 20, 2024 (hereinafter, the "Incident"). MF takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter is to provide an update to the preliminary notice of the Incident sent to your office on December 20, 2024, which was sent in an effort to provide timely notice to the Washington State Attorney General's office while the forensic investigation of the incident is still ongoing.

1. Nature of the Incident

On or about November 20, 2024, MF detected unusual activity within its systems. Upon discovery of this incident, MF promptly engaged a specialized third-party cybersecurity and IT firm to assist with securing the computer systems in question, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensics investigation determined that certain data contained in the computer systems was accessible by an unauthorized actor.

Based on these findings, MF performed data mining on the affected systems to identify the specific individuals and the types of information that may have been compromised. Following that internal review, MF has worked to obtain valid and updated contact information for potentially affected individuals. On April 23, 2025, MF finalized the list of individuals to notify.

2. Number of Washington residents affected.

A total of seventy three (73) Washington resident(s) that may have been potentially affected by this incident. While the number of incident-impacted individuals fall below the threshold for regulatory notice, we provide this notice for the sake of updating the Attorney General's Office with the final number. Notification letters to these individuals will be mailed on Monday, April 28, 2025, by first class mail. A sample each copy of the notification letter are included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

MF is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, MF moved quickly to investigate and respond to the Incident, assessed the security of its systems, and is performing the necessary steps to determine the potentially affected individuals to provide notices. MF has engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, MF has implemented multi-factor authentication (MFA) and additional security measures. Lastly, MF informed our law firm and is currently working towards identifying the potentially affected individuals in preparation for notice.

Although MF is not aware of any actual or attempted misuse of the affected personal information, MF offered twelve (12) months of complimentary credit monitoring and identity theft restoration services through Cyberscout to all individuals to help protect their identity. Additionally, MF provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

Marine Floats remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A

0000073

Marine Floats
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS800

0_0000073

Parent/ Guardian of
[redacted]

April 28, 2025

Re: Data Security Incident

Dear Parent/ Guardian of [redacted]

Marine Floats LLC ("Marine Floats") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your child's sensitive personal information. While we are unaware of any fraudulent misuse of your child's personal information, at this time, we ae providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your child's information.

What Happened? On or about November 20, 2024, Marine Floats detected unusual activity within its systems. Upon discovery of this incident, Marine Floats promptly engaged a specialized third-party cybersecurity and IT firm to assist with securing the computer systems in question, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensics investigation determined that certain data contained in the computer systems was accessible by an unauthorized actor.

Based on these findings, Marine Floats performed data mining on the affected systems to identify the specific individuals and the types of information that may have been compromised. Following that internal review, Marine Floats has worked to obtain valid and updated contact information for potentially affected individuals. On April 23, 2025, Marine Floats finalized the list of individuals to notify.

What Information Was Involved? Based on the investigation, the following information related to you may have been subject to unauthorized access: Date of Birth.

What We Are Doing. Marine Floats takes security of its information very seriously, and has taken steps to prevent a similar event from occurring in the future. Since the discovery of the incident, Marine Floats moved quickly to investigate, respond, and confirm the security of our computer systems. Specifically, Marine Floats engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the incident. Additionally, Marine Floats has implemented multi-factor authentication (MFA) and additional security measures.

In response to the incident, we are providing the parents of impacted minors with access to **Cyber Monitorin**g services for you and your minor child at no cost to you for 12 months. Cyber monitoring will look out for yours and your child's personal data on the dark web and alert you if your personally identifiable information or your child's is found online. These services will be provided by Cyberscout, a TransUnion company, specializing in fraud assistance and remediation services.

What You Can Do. To enroll in Cyber Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]

Once you have completed the enrollment for yourself, click on your name in the top right of your dashboard and then "Add Family Member" to enroll your child. To complete the child's enrollment, click on the child's name and provide the requested information for monitoring. In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and an email account and will require enrollment by parent or guardian first. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We would like to reiterate that, at this time, there is no evidence that your child's information was misused. However, we encourage you to take full advantage of the services offered. Please review the enclosed *Additional Resources to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

For More Information. If you have any questions or concerns not addressed in this letter, please call 1-800-405-6108 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time, Monday through Friday, excluding U.S. national holidays.

Marine Floats sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

MARINE FLOATS LLC

0000073

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts. We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies. You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze. You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert. You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission. For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information. Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002, Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554, Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554, Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241, Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069, Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788, Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
TransUnion	P.O. Box 1000, Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000, Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160, Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

Marine Floats
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS800

0000072

0_0000072

[redacted]

April 28, 2025

Re: Data Security Incident

Dear [redacted]

Marine Floats LLC ("Marine Floats") is writing to inform you of a recent data security incident that may have resulted in unauthorized access to your sensitive personal information. We are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

What Happened? On or about November 20, 2024, Marine Floats detected unusual activity within its systems. Upon discovery of this incident, Marine Floats promptly engaged a specialized third-party cybersecurity and IT firm to assist with securing the computer systems in question, as well as to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensics investigation determined that certain data contained in the computer systems was accessible by an unauthorized actor.

Based on these findings, Marine Floats performed data mining on the affected systems to identify the specific individuals and the types of information that may have been compromised. Following that internal review, Marine Floats has worked to obtain valid and updated contact information for potentially affected individuals. On April 23, 2025, Marine Floats finalized the list of individuals to notify.

What Information Was Involved? Based on the investigation, the following information related to you may have been subject to unauthorized access: Date of Birth, Social Security Number, Driver License or State ID Number.

What We Are Doing. Marine Floats takes security of its information very seriously, and has taken steps to prevent a similar event from occurring in the future. Since the discovery of the incident, Marine Floats moved quickly to investigate, respond, and confirm the security of our computer systems. Specifically, Marine Floats engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the incident. Additionally, Marine Floats implemented multi-factor authentication (MFA) and additional security measures.

In light of the incident, Marine Floats is providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Additional Resources To Help Protect Your Information*, to learn more about how to help protect against the possibility of information misuse.

How do I activate the complimentary services?

Visit **https://bfs.cyberscout.com/activate** to activate and take advantage of your identity monitoring services.

*You have until **July 29, 2025** to activate your identity monitoring services.*

Membership Number: [redacted]

In order for you to receive the monitoring services described above, you must activate within 90 days from the date of this letter. The activation requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for identity monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

We encourage you to take full advantage of the services offered.

For More Information. If you have any questions or concerns not addressed in this letter, please call 1-800-405-6108 (toll free) Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time, Monday through Friday, excluding U.S. national holidays.

Marine Floats sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

MARINE FLOATS LLC

0000072

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts. We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies. You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze. You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert. You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission. For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information. Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002, Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554, Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554, Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241, Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069, Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788, Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
TransUnion	P.O. Box 1000, Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000, Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160, Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.

December 20, 2024

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Submission:

Attorney General Bob Ferguson
1125 Washington St SE
PO Box 40100
Olympia, WA 98504
(360) 753-6200
Email: SecurityBreach@atg.wa.gov

Re: Cybersecurity Incident Involving Marine Floats LLC

Dear Attorney General Ferguson:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Marine Floats LLC ("MFL"), a business that designs, builds, and maintains custom waterfront structures, located in 313 East F St., Tacoma, WA 98421, with respect to a recent cybersecurity incident that was first discovered by MFL on or around November 20, 2024 (hereinafter, the "Incident"). MFL takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter is a preliminary notice of the Incident in an effort to provide timely notice to the Washington State Attorney General's office while the forensic investigation of the incident is still ongoing.

1. Nature of the Incident

On or around November 20, 2024, MFL discovered the Incident when an unauthorized access to its system was detected. Upon discovery of the incident, MFL promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation is still ongoing. MFL will provide an update to the Washington State Attorney General's office when the forensic investigation is completed.

2. Number of Washington residents affected.

As of the date of this letter, the total number of Washington resident(s) that may have been potentially affected by this incident is not yet determined. When MFL determines the total number of incident-impacted individuals, MFL will provide an update to the Washington State Attorney General's office and mail notices to the incident-impacted individuals.

3. Steps taken in response to the Incident.

MFL is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, MFL moved quickly to investigate and respond to the Incident, assessed the security of its systems, and is performing the necessary steps to determine the potentially affected individuals to provide notices. MFL has engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, MFL has implemented multi-factor authentication (MFA) and additional security measures. Lastly, MFL informed our law firm and is currently working towards identifying the potentially affected individuals in preparation for notice.

4. Contact information

MFL remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

December 20, 2024

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via Online Submission:

Attorney General Bob Ferguson
1125 Washington St SE
PO Box 40100
Olympia, WA 98504
(360) 753-6200
Email: SecurityBreach@atg.wa.gov

Re: Cybersecurity Incident Involving Marine Floats LLC

Dear Attorney General Ferguson:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Marine Floats LLC ("MFL"), a business that designs, builds, and maintains custom waterfront structures, located in 313 East F St., Tacoma, WA 98421, with respect to a recent cybersecurity incident that was first discovered by MFL on or around November 20, 2024 (hereinafter, the "Incident"). MFL takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter is a preliminary notice of the Incident in an effort to provide timely notice to the Washington State Attorney General's office while the forensic investigation of the incident is still ongoing.

1. Nature of the Incident

On or around November 20, 2024, MFL discovered the Incident when an unauthorized access to its system was detected. Upon discovery of the incident, MFL promptly engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the incident. The forensic investigation is still ongoing. MFL will provide an update to the Washington State Attorney General's office when the forensic investigation is completed.

2. Number of Washington residents affected.

As of the date of this letter, the total number of Washington resident(s) that may have been potentially affected by this incident is not yet determined. When MFL determines the total number of incident-impacted individuals, MFL will provide an update to the Washington State Attorney General's office and mail notices to the incident-impacted individuals.

3. Steps taken in response to the Incident.

MFL is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, MFL moved quickly to investigate and respond to the Incident, assessed the security of its systems, and is performing the necessary steps to determine the potentially affected individuals to provide notices. MFL has engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, MFL has implemented multi-factor authentication (MFA) and additional security measures. Lastly, MFL informed our law firm and is currently working towards identifying the potentially affected individuals in preparation for notice.

4. Contact information

MFL remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or 312-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das