BRUNSWICK™
Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Re: Notification of Data Breach Incident

Dear <<Name 1>>,

Brunswick Corporation ("**Brunswick**" or "**we**") understands the importance of cybersecurity and protecting your sensitive personal data. As you may know, Brunswick was the victim of an Information Technology (IT) security incident earlier this year. In response to this incident, we conducted a comprehensive and thorough investigation. Although we identified that your personal data was impacted by this incident, **we have no reason to believe that any of your personal data has been misused, or will be misused in the future**. However, out of an abundance of caution, we are providing you and other individuals potentially affected by this incident with complimentary credit monitoring services.

What Happened

On or around June 10, 2023, we discovered that a third party had gained unauthorized access to certain systems in our IT environment. In response, we immediately deployed security measures to contain and mitigate this threat, and we retained a leading incident response team to accelerate our recovery efforts. Because of the substantial security controls we implemented prior to this incident, we were able to contain the threat and return to a normal state of business within a short time. However, as part of our investigation into this incident, we discovered that the perpetrator of the attack accessed certain Brunswick files and records. To address this issue, we hired a data consultant to undertake a comprehensive review of each of these files and records to identify whether any of them contained personal data. They recently finished this review and thereafter we began notifying relevant individuals who could have been affected by this incident.

What Information Was Involved

We have discovered the unauthorized third-party obtained access to limited e-mail accounts and unstructured files that contained certain personal data. These documents were either e-mail communications or files used by Brunswick to provide benefit programs to our employees and their family members (e.g., health and wellness programs, retirement plans), to assess worker and contractor eligibility, and for tax filing and similar business purposes. Accordingly, this personal data relates to Brunswick employees and potentially their beneficiaries and dependents, customers, and contractors, and may include one or more of the following types of personal data: *names; mailing addresses; telephone numbers; social security numbers, driver's license numbers, and similar government-provided identification documentation; birth certificates (if provided for employment or work verification purposes), payment card information; healthcare and health insurance-related data, and account access credentials*. To be clear, Brunswick's personnel and benefits systems, such as Workday, were not compromised during this incident.

What We Are Doing / How We Responded

We take this event and the security of information in our care seriously. Given the comprehensive information security program that Brunswick had established prior to this incident, we were able to return to a normal state of operations in a timely manner. Our IT security team responded promptly and immediately deployed security measures to contain and mitigate this threat, including pausing operations in some locations, engaging leading security experts, coordinating with relevant law enforcement agencies, and engaging with relevant data protection regulatory authorities. In addition, we undertook and completed a thorough investigation of this incident, and we have taken action to help prevent future occurrences.

Credit Monitoring Services

To help address any concerns you may have, Brunswick will provide you and your immediate family members with complimentary credit monitoring and identity theft protection services for 24 months, offered through *Experian IdentityWorks*™. If you are a current employee, you may already have access to these services as part of our benefits program. Please contact our call center listed below for more information about how to access and enroll in these services.

What You Can Do

Because of the measures and steps that Brunswick took following this incident, **there is no indication that your personal data has been misused or will be misused in the future**. However, there are several steps that you can take to better protect yourself and your personal data more generally. See the attachment for additional information with respect to certain security services that may be available to you.

Point of Contact / Call Center

We have established a dedicated call center to answer questions you may have about this incident, which you can reach at **888-722-0568**, Monday – Friday, 9:00 am to 9:00 pm (Eastern Standard Time).

* * * * * * * * * *

We deeply regret that this incident occurred, and we thank you for your attention to this matter.

Sincerely,

The Brunswick Privacy Office

Additional Data Security Information

It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any 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 companies. To order your annual free credit report, please visit www.annualcreditreport.com, call toll free at 1-877-322-8228 or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.consumer.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the three nationwide credit reporting companies is as follows:

- Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111.
- Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742.
- TransUnion, PO Box 2000, Chester, PA 19016, https://www.transunion.com, 1-800-916-8800.

When you receive your credit report: (i) review it carefully, (ii) look for accounts you did not open, (iii) look in the "personal information" section for any inaccuracies in your information (such as home address and Social Security Number). You should also look in the "inquiries" section for names of creditors from whom you have not requested credit. You should notify the consumer reporting agencies immediately of any inaccuracies in your report or if you see anything you do not understand. The consumer reporting agency and staff will review your report with you. 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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows: Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), http://www.ftc.gov/idtheft.

If you are a resident of California, Connecticut, Maryland, or Massachusetts, you may contact and obtain information from your state Attorney General at the following:

- California Department of Justice, Office of Privacy Protection, PO Box 944255, Sacramento, CA 94244-2550, 1-800-952-5225, www.oag.ca.gov/privacy.
- Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.
- Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 or 1-410-576-6300, www.marylandattorneygeneral.gov.
- North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, https://ncdoj.gov/, 1-919-716-6400 or 1-877-566-7226.
- Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/contact-the-attorney-generals-office.

If you are a resident of Massachusetts, you have the right to file and obtain a copy of a police report, are allowed to place, without charge, a security freeze on your credit reports, and may contact and obtain information from and/or report identity theft to your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html.

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 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with 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.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a personal identification number ("PIN") that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security freeze, potential creditors and other third

parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit. There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses listed above.

To request a security freeze, you will need to provide the following information: (i) Your full name (including middle initial as well as Jr., Sr., II, III, etc.), (ii) Social Security number, (iii) Date of birth, (iv) If you have moved in the past five years, provide the addresses where you have lived over the prior five years, (v) Proof of current address such as a current utility bill or telephone bill, (vi) A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.), (vii) If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act (the "FCRA"), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The Federal Trade Commission has published a list of the primary rights created by the FCRA, and the article is available at (https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The Federal Trade Commission's list of FCRA rights includes the following:

You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request. Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months. You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days, if you are on welfare, or if your report is inaccurate because of fraud, including identity theft. You have the right to ask for a credit score. You have the right to dispute incomplete or inaccurate information. Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Consumer reporting agencies may not report outdated negative information. Access to your file is limited. You must give your consent for reports to be provided to employers. You may limit "prescreened" offers of credit and insurance you receive based on information in your credit report. You may seek damages from violators. Identity theft victims and active-duty military personnel have additional rights.

Note: The delivery of this notice has not been delayed as a result of a law enforcement investigation.