

Brunswick Corporation Addresses Previously Reported Data Security Incident

METTAWA, Ill., Dec. 21, 2023 (GLOBE NEWSWIRE) -- Brunswick Corporation ("Brunswick") understands the importance of protecting personal data and retaining the trust of its customers and employees. Unfortunately, as noted in previous disclosures, Brunswick was the victim of a data security incident in June 2023. In response to this incident, Brunswick conducted a comprehensive and thorough investigation and identified that a limited amount of sensitive personal data in its custody or control was impacted by this incident. However, Brunswick has no reason to believe that any personal data has been misused or will be misused in the future.

What Happened? In June 2023, Brunswick discovered that a third party had gained unauthorized access to certain systems in its information technology (IT) environment. Brunswick immediately deployed security measures to contain and mitigate this threat and retained a leading incident response team to accelerate its recovery efforts. Brunswick proactively notified relevant law enforcement agencies and data protection authorities about this incident. Because of the substantial security controls implemented prior to this incident, Brunswick was able to quickly contain the threat and return to a normal state of business operations. In addition, Brunswick hired a data consultant to undertake a comprehensive review of the files and records impacted by this incident to identify whether any of them contained personal data. The consultants recently finished this review and thereafter Brunswick began notifying relevant individuals who could have been affected by this incident.

What Personal Data Was Impacted? As part of its thorough internal investigation, Brunswick discovered that an unauthorized third-party obtained access to a limited number of e-mail boxes and unstructured files that contained certain sensitive personal data.

What You Can Do. Based on the measures that Brunswick implemented, there is no indication that any sensitive personal data involved in this incident has been misused or will be misused in the future. However, out of an abundance of caution, Brunswick is providing certain individuals potentially affected by this incident with complimentary credit monitoring and identity theft protection services, where appropriate.

Current Employees: If you are a current Brunswick employee whose personal data was affected by the incident, you will receive a separate notice in the mail from Brunswick that provides instructions on how you can enroll in these services.

Customers/Suppliers/Former Employees: If you are a customer, supplier, or former employee of Brunswick, please inquire (via the phone number in the "For More Information" paragraph below) as to whether your sensitive personal data was subject to this incident and whether you are eligible to enroll in complimentary credit monitoring services.

For More Information. Brunswick has 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 (EST). More information is available at: <https://www.brunswick.com/securityincident>. You can also request to know which personal data Brunswick retains about you by submitting a Subject Access Request at <https://www.brunswick.com/dsar>.

Data Protection Officer – European Economic Area:

Brunswick's Data Protection Officer's contact information is as follows:

Felix Wittern – FieldFischer

dpo.brunswick@fieldfisher.com

Source: Brunswick Corporation, 26125 N. Riverwoods Blvd., Suite 500, Mettawa, Illinois 60045

Lee

Gordon –

Vice President - Corporate Communications, Public Relations & Public Affairs

M: (904) 860-8848 | O: (847) 735-4003



Source: Brunswick Corporation