Carnival Cruise Brings Multistate Data Breach into Port

Paul L. Singer, Beth Bolen Chun

June 28, 2022

Even as states continue to pass comprehensive privacy laws, Attorneys General remain active enforcing their data breach laws and utilizing their deceptive trade practice authority in the privacy space. Just last week, 46 State AGs signed on to a settlement, which took the form of an Assurance of Voluntary Compliance, with international cruise corporation Carnival for its 2019 data breach. This breach of employee email accounts purportedly exposed sensitive personal information contained in email contents, thereby impacting state consumers. The payment to the states is $1.25 million total.

While this settlement joins a long list of AG privacy cases, it serves as a useful roadmap for companies wishing to stay on top of what AGs expectations are for data security, and what type of enforcement terms you can expect if you suffer a breach.

In its agreement, Carnival has agreed to comply with state laws prohibiting unfair and deceptive trade practices, as well as specific data security and breach notification laws, specifically in connection with securing Personal Information (as defined by state statutes) against Security Incidents, defined as confirmed unauthorized access to or acquisition of a Consumer's personal information owned, licensed, or maintained by Carnival. It also agrees to comply with consumer protection acts with respect to representations regarding privacy and security of personal information.

Within 180 days of the effective date Carnival must maintain a comprehensive information security program, appropriate to the size and complexity of operations, nature and scope of activities, and the sensitivity of personal information. Carnival must employ a Chief Information Security Officer and must further must provide security awareness and privacy training to all personnel with access to the network or responsibility for personal information every year and after hiring. Carnival also must update its written incident response and data breach notification plan to ensure compliance addressing preparation, detection and analysis, containment, eradication, and recovery workflows.

Carnival must further develop, implement and maintain retention of personal information policies, use email filtering and protection, establish encryption policies, and maintain an appropriate system to collect logs and monitor network activity through and establish policies to analyze security events and real time. Carnival must implement appropriate policies to audit accounts, ensure protected passwords, multifactor authentication for remote access, firewall policies, penetration testing, and conduct an annual risk assessment. The company also must obtain a risk assessment from a third party within 18 months of the effective date and provide a copy to the State of Washington for review.

While several of the specific provisions expire after 5 years, it should be apparent that State AGs will

demand detailed compliance programs and continued oversight if they find a lapse in security practices. Ensuring you have a detailed security program now and continually seeking ways to enhance your security practices are valuable ways to minimize AG scrutiny later. Note also that some of the injunctive terms are broadly applicable even beyond the specific incident in question, which potentially can subject the company to heightened penalties should there be another, albeit unrelated, security incident.

* * * *

Join us tomorrow for State Attorneys General 102. This short 30-minute webinar picks up where State Attorneys General 101 left off and answers a number of questions regarding:

- Pre-suit/investigation notice requirements for Attorneys General
- Additional information on the scope of Attorneys General investigative authority and how to challenge an investigation
- Consumer Complaints: differences among the AGs on handling and use

Register here