FOR IMMEDIATE RELEASE
June 23, 2022
#22-18

CONTACT: Samantha Fisher
615.741.5860
Samantha.Fisher@ag.tn.gov

TENNESSEE JOINS $1.25 MILLION MULTISTATE SETTLEMENT OVER 2019 CARNIVAL CRUISE LINE DATA BREACH

Nashville – Attorney General Herbert H. Slatery III announced that Tennessee, along with 45 other attorneys general, has obtained a $1.25 million multistate settlement with Florida-based Carnival Cruise Line after a 2019 data breach that involved the personal information of approximately 180,000 Carnival employees and customers nationwide. Tennessee will receive $19,855.20 from the settlement.

In March 2020, Carnival publicly reported a data breach in which an unauthorized actor gained access to certain Carnival employee e-mail accounts. The breach included names, addresses, passport numbers, driver's license numbers, payment card information, health information, and a relatively small number of Social Security Numbers. In Tennessee, more than two thousand Carnival employees were impacted.

Breach notifications sent to attorneys general offices stated that Carnival first became aware of suspicious email activity in late May of 2019—approximately 10 months before Carnival reported the breach. A multistate investigation ensued, focusing on Carnival's email security practices and compliance with state breach notification statutes.

"Unstructured" data breaches like the Carnival breach involve personal information stored via email and other disorganized platforms. Businesses lack visibility into this data, making breach notification more challenging—and consumer risk rises with delays.

"Unfortunately, we live in a world where data breaches will continue to happen," said General Slatery. "What's not inevitable is how a company reacts. We hope this serves as a reminder: you are required by state law to promptly notify those affected."

Under the settlement, Carnival has agreed to a series of provisions designed to strengthen its email security and breach response practices going forward. Those include:

- Implementation and maintenance of a breach response and notification plan;
- Email security training requirements for employees, including dedicated phishing exercises;
- Multi-factor authentication for remote email access;
- Password policies and procedures requiring the use of strong, complex passwords, password rotation, and secure password storage;

- Maintenance of enhanced behavior analytics tools to log and monitor potential security events on the company's network; and
- Consistent with past data breach settlements, undergoing an independent information security assessment.

Connecticut co-led the multistate investigation with Florida and Washington, assisted by Alabama, Arizona, Arkansas, Ohio, and North Carolina, and joined by Alaska, Colorado, Delaware, the District of Columbia, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, New York, North Dakota, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Virginia, West Virginia, Wisconsin, and Wyoming.

###