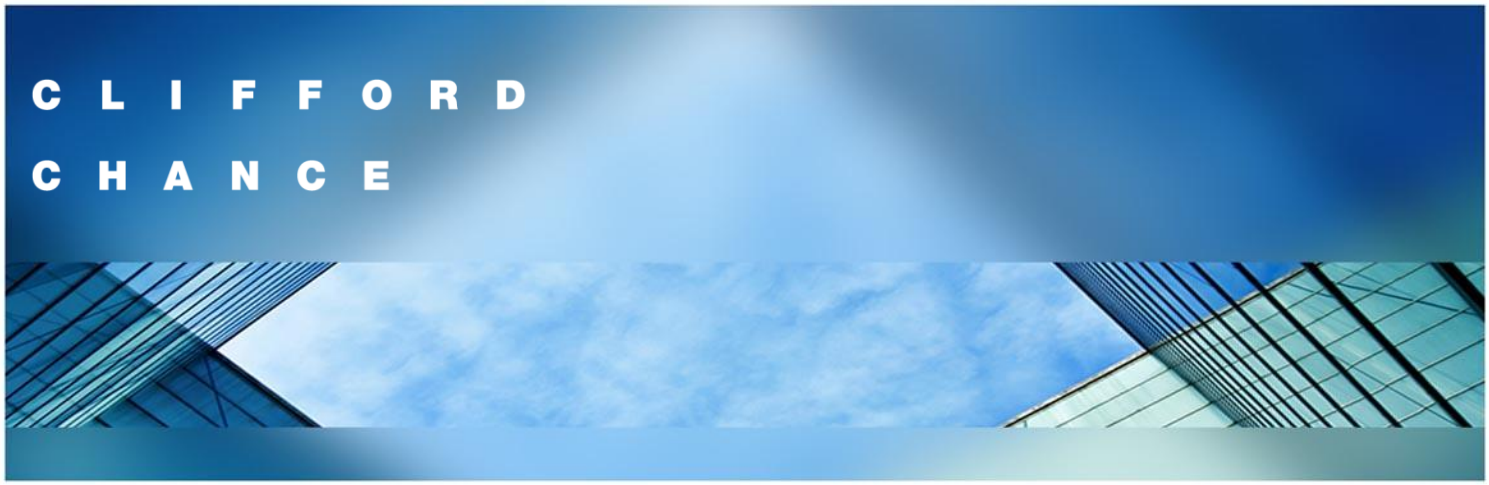

NYDFS PENALIZES CRUISE SHIP OPERATOR FOR FAILING TO PREVENT AND TIMELY REPORT CYBERATTACKS

On June 23, 2022, the New York Department of Financial Services ("NYDFS") issued a Consent Order finding that cruise ship operator Carnival Corporation violated the Department's cybersecurity regulation by failing to implement required policies and procedures as well as report several cyber incidents that the company experienced. The enforcement action signals DFS's determination to ensure all licensed entities—including victims of cyberattacks—fully protect sensitive customer and employee data by rigorously adhering to NYDFS's cybersecurity regulation.

Key issues

- NYDFS found that Carnival Corporation violated the Department's cybersecurity regulation.
- The cruise line is under the purview of the agency via its insurance business.
- DFS licensees may be subject to penalties for cyber breaches and failure to protect sensitive data even if financial services comprise only a small portion of their overall operations.

OVERVIEW OF THE NYDFS CYBERSECURITY REGULATION

Adopted in March 2017, the NYDFS Cybersecurity Requirements for Financial Services Companies (the "Regulation") require Covered Entities–including banks, insurance companies, and other institutions licensed or regulated by NYDFS, along with third-party service providers–to put in place a risk-based cybersecurity program that provides appropriate protection of the entity's information systems and data. This program must include written policies and procedures, risk assessment activities, and other industry-standard cybersecurity program elements. One such control emphasized by the Regulation is the use of multi-factor authentication ("MFA"), a requirement that is only excused when the Chief Information Security Officer ("CISO") "approve[s] in writing the use of . . . reasonably equivalent or more secure access controls." The CISO must also certify annually to NYDFS that the Covered Entity's program is compliant and maintain supporting documentation for five years for examination by the regulator.[1]

THE CARNIVAL CONSENT ORDER

NYDFS's Consent Order discussed four cybersecurity incidents affecting Carnival Corporation that exposed customer and employee personal information. While Carnival Corporation's primary business is operating cruise ships, it also offers life,

[1] For a discussion of the Regulation and its requirements, see our briefing here.

accident, and health insurance pursuant to a license from NYDFS—activities that brought it within the scope of the Regulation. Most of the incidents arose from various ransomware attacks whereby hackers infiltrated Carnival's information system through phishing emails sent to and from company email accounts.[2]

According to the Order, Carnival became aware of the first cyber incident after an internal investigation revealed that unauthorized parties had gained access to 124 employee email accounts hosted on their software platform and then used that access to send a series of phishing emails to other employees. The unauthorized access led to the exposure of personal information of consumers and employees, including hundreds of New York residents who had their names, addresses, passport numbers, and driver's license numbers exposed. At the time of this first incident, the company had not yet implemented multi-factor authentication on its software platform, even though this was a requirement of the Regulation. Additionally, though Carnival became aware of the incident in May 2019, they did not report it to NYDFS until April 2020—despite the requirement that cyber incidents be reported to the agency within 72 hours. The NYDFS Order noted that this was due to the fact that Carnival's incident response plan did not include reference to the Regulation's notification requirement.

Carnival experienced three additional cyber incidents from August 2020 to March 2021 that followed a similar pattern: a threat actor gained unauthorized access to Carnival's IT system, usually as the result of a phishing scheme, leading to the exposure of consumer personal information, including sensitive data like social security numbers and private health data.

Because Carnival is considered a Covered Entity, NYDFS expects it to meet the standards set by the Regulation. This includes implementation of MFA and cybersecurity awareness training for all personnel, which NYDFS concluded was inadequate due to the occurrence of four cyber incidents within four years—at least some of which resulted from phishing attacks. The Order also pointed out that Carnival's CISO had certified compliance with the Regulation for 2018, 2019, and 2020—certifications that were improper given the cyber events and the underlying noncompliance that caused them.

Due to the violations identified in the Order, Carnival agreed to a $5 million penalty. Notably, this penalty was four times higher than the $1.25 million combined settlement Carnival reached the previous day with 45 states for failure to timely notify victims of the breach. Carnival also agreed to surrender its insurance licenses issued by NYDFS and cease selling insurance in New York. The Order marks the fourth time NYDFS has used the Regulation to fine a corporation for inadequate cybersecurity programs.[3]

CONCLUSION & TAKEAWAYS

NYDFS's Cybersecurity Regulation can create substantial obligations to safeguard systems and report data breaches for licensees, even when the licensee's core business is not related to the financial services industry. Businesses that NYDFS supervises for even a small portion of their business should take care to

[2] One area of focus for NYDFS is vulnerability to ransomware attacks. Last year, NYDFS released Ransomware Guidance highlighting specific cybersecurity controls that companies should implement. For more information about this guidance, see our briefing here.

[3] For information about other enforcement actions brought by NYDFS under this regulation, see our coverage here.

implement and maintain cybersecurity practices that satisfy the Regulation, including MFA, employee training to avoid phishing attacks, and an incident response plan that incorporates the requirement to alert NYDFS within 72 hours of discovering a breach. Failure to comply with the Regulation can result in costly fines and the inability to continue conducting financial activities regulated by the NYDFS.

CONTACTS

Celeste Koeleveld
Partner

T +1 212 878 3051
E celeste.koeleveld
@cliffordchance.com

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Daniel Silver
Partner

T +1 212 878 4919
E daniel.silver
@cliffordchance.com

Thomas Chapman
Associate

T +1 202 912 5921
E thomas.chapman
@cliffordchance.com

Brian Yin
Associate

T +1 212 878 4980
E brian.yin
@cliffordchance.com

Will Lanier
Summer Law Clerk

T +1 212 880 5815
E will.lanier
@cliffordchance.com

Naomi Flores Urrutia
Summer Law Clerk

T +1 212 880 5755
E naomi.floresurrutia
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.