

## **NYDFS FINES HEALTH INSURER EYEMED \$4.5 MILLION FOR CYBERSECURITY VIOLATIONS AFTER MANDATORY SELF-REPORT**

On October 18, 2022, the New York Department of Financial Services (“NYDFS”) announced a \$4.5 million penalty against health insurer EyeMed Vision Care LLC (“EyeMed”) for violations of the Department’s Cybersecurity Regulation that contributed to a July 1, 2020 data breach that exposed sensitive, non-public consumer health data of New York residents. Notably, NYDFS learned about the breach after EyeMed reported the incident, as required by the Cybersecurity Regulation. The penalty is a reminder to companies in scope of the regulation to make sure to review their compliance before an incident, a costly lesson more and more companies are learning from NYDFS.

### **OVERVIEW OF THE NYDFS CYBERSECURITY REGULATION**

New York’s Cybersecurity Regulation requires NYDFS-regulated entities to implement a risk-based cybersecurity program that protects the entity’s information systems and data. This program must be informed by periodic risk assessments and include certain enumerated cybersecurity controls, including use of multi-factor authentication, user access controls, data retention and disposal processes, and incident response protocols. Entities must designate a Chief Information Security Officer (“CISO”), who must certify compliance with these requirements annually. In addition, the Cybersecurity Regulation requires entities that suffer a material data breach to report the incident to NYDFS within 72 hours, one of the most aggressive reporting timelines in the world.<sup>1</sup>

EyeMed, one the largest vision insurance companies in the US, is licensed by NYDFS to sell health insurance in New York State. This licensure brings the company in scope of the NYDFS Cybersecurity Regulation.

<sup>1</sup> For more information on NYDFS’s Cybersecurity Regulation, see our briefing [here](#).

## THE EYEMED CONSENT ORDER

According to the Consent Order, EyeMed reported the data breach to NYDFS on October 9, 2020. On July 1, 2020, EyeMed discovered that an unauthorized user had gained access to an email account used by the insurer to process enrollment and communicate updates to group clients. The intrusion had begun approximately a week earlier on June 24, and had allowed the attacker to access and view emails and attachments from the past six years and that contained consumer non-public health information. According to the Consent Order, EyeMed's investigation was unable to determine how the attacker gained access to the mailbox, but the insurer believes that the triggering event was likely a phishing scheme.<sup>2</sup>

After receiving EyeMed's report, NYDFS investigated the licensed insurer and determined that at the time of the attack, EyeMed had not implemented several controls required by the Cybersecurity Regulation. These missing controls included:

- **Missing Multi-Factor Authentication.** At the time of the attack, EyeMed was in the process of rolling out multi-factor authentication for its email accounts—but the affected account had not yet been included in the roll-out.
- **Inadequate Risk Assessments.** EyeMed engaged third-party vendors to conduct periodic audits of IT controls and reviews of enterprise risk management. However, NYDFS found these audits and reviews did not meet the standards set out in the Cybersecurity Regulation—as evidenced by the fact that none of the assessments addressed the risk of consumer non-public information stored within the affected mailbox.
- **Overbroad User Access Privileges.** Nine EyeMed employees shared login credentials for the affected mailbox, and the email account had a weak password.
- **Lack of Secure Disposal.** EyeMed did not have data minimization and disposal processes that applied to the affected mailbox, resulting in the account holding more non-public consumer health data than the company may have needed for its operations, increasing the risk to consumers.

According to NYDFS, had these controls been in place, the attack would have been at least partially mitigated, if not completely avoided.

As required by the Cybersecurity Regulation, EyeMed certified compliance with the requirements for each year from 2017–2020. According to the Consent Order, EyeMed asserted to NYDFS during the Department's investigation that the insurer had made the certifications in good faith. NYDFS rejected this "good faith" argument as a defense, however, finding that EyeMed had not in fact been in compliance when it had made the certifications, and thus those certifications were improper.

---

<sup>2</sup> The NYDFS Consent Order does not discuss the timing of EyeMed's notification, but it is worth noting that EyeMed's notification to NYDFS on October 9—over three months after it discovered the breach on July 1—appears not to comply with the Cybersecurity Regulation's 72 hour breach notification requirement. It is not clear why the delay occurred (or whether and how NYDFS took issue with the delay), but it seems like this may have been another area of noncompliance.

In addition to the \$4.5 million fine, the Consent Order requires the insurer to implement several measures to remediate identified deficiencies. These measures include conducting a comprehensive risk assessment that meets the standard of the Cybersecurity Regulation, along with a “detailed Action Plan” describing the steps EyeMed would take to address any identified deficiencies.

## **TAKEAWAYS**

While the Consent Order itself is straightforward, the EyeMed enforcement action nevertheless highlights several key takeaways for companies regulated by NYDFS.

First, several of the specific deficiencies identified have been a common thread in recent enforcement actions, including lack of multi-factor authentication<sup>3</sup> and inadequate risk assessments.<sup>4</sup> All companies in scope of the Cybersecurity Regulation should know that they need to have these controls in place when NYDFS comes knocking.

Second, the size of the fine is a reminder both that NYDFS fines can be quite hefty, but also that cooperation and timely remediation can help mitigate the penalties. The Consent Order specifically includes a paragraph recognizing EyeMed’s “commendable cooperation” during the Department’s investigation and the insurer’s “commitment to remediation” with “significant financial and other resources.” While the \$4.5 million penalty is certainly a significant sum, this recognition in the Consent Order suggests that NYDFS may have considered and imposed an even larger fine absent EyeMed’s cooperation and remediation efforts.

Finally, the sequence of events leading up to the investigation and eventual fine is a reminder to companies to be ready when they make reports. Companies should always ensure that they fulfill mandatory reporting obligations, but they need to be aware that such reports will likely trigger investigations—sometimes by multiple government bodies.<sup>5</sup> As a result, preparing early is key—while incident response is paramount following an attack, a company must also consider the legal and regulatory fallout, taking into account key issues such as legal privilege, recordkeeping, and remediation.

---

<sup>3</sup> Lack of multi-factor authentication was one of the main issues in the Department’s June 23 Consent Order with cruise ship operator Carnival Corporation. For more on that penalty, see our briefing [here](#).

<sup>4</sup> Inadequate risk assessments were one of the cybersecurity deficiencies that led to the Department’s August 1 Consent Order with cryptocurrency trading platform operator Robinhood. For more on that penalty, see our briefing [here](#).

<sup>5</sup> New York state [fined](#) EyeMed \$600,000 in January 2022 for the same breach, citing violations of the NY SHIELD Act.

## 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

**Devika Kornbacher**  
Partner

**T** +1 212 878 3424  
**E** devika.kornbacher  
@cliffordchance.com

**Dennis Manfredi**  
Partner

**T** +1 212 878 3226  
**E** dennis.manfredi  
@cliffordchance.com

**Daniel Silver**  
Partner

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

**Eugene Bengner**  
Counsel

**T** +1 212 878 8033  
**E** eugene.bengner  
@cliffordchance.com

**Brian Yin**  
Associate

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

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

[www.cliffordchance.com](http://www.cliffordchance.com)

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

© Clifford Chance 2022

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.