Published: January 30, 2024

New Cybersecurity Breach Notice Requirement for Entities Licensed in New York

Seth Bracelin | Millenium Insurance Group | (717) 354-4774 | sbracelin@millig.com

A recent amendment to 23 NYCRR Part 500, commonly referred to as the "Cybersecurity Regulation," now requires entities and individuals licensed under the New York Insurance Law to notify the New York Department of Financial Services ("DFS") within 72 hours after learning of a cybersecurity incident that has occurred at a third-party service provider. Although the original regulation required notice within 72 hours, the updated regulations require notice where a third-party service provider has a cybersecurity incident. These changes to the notice and reporting provisions went into effect on December 1, 2023.

Background

DFS enacted the Cybersecurity Regulation in 2017 establishing cybersecurity requirements that apply to, among others, any entity or individual who is required to be licensed under the New York Insurance Law. The Cybersecurity Regulation was amended in 2020, and again more recently in November 2023 (the "Amendment"). Insurance agents, producers and brokers who are licensed (or should be licensed) to sell life and health insurance in New York are Covered Entities under the Cybersecurity Regulation and are required, among other things, to provide timely notice of a cybersecurity incident to DFS.

Changes Under the Amendment

While the Cybersecurity Regulation has been around since 2017, the Amendment made some notable changes to the definition of a cybersecurity incident and to the notice provisions that apply to Covered Entities. It should be noted that this Bulletin does not discuss the Cybersecurity Regulation in its entirety, as it has existed for some time; rather its focus is to provide you with important changes that were made under the Amendment. In short, agents, producers and brokers must (as of December 1, 2023) notify DFS of a cybersecurity incident even if that incident took place at one of their vendors.

This document is designed to highlight various employee benefit matters of general interest to our readers. It is not intended to interpret laws or regulations, or to address specific client situations. You should not act or rely on any information contained herein without seeking the advice of an attorney or tax professional. © Emerson Rogers, LLC. All Rights Reserved.
CA Insurance License #0C94240.

Definition of Cybersecurity Incident

The Amendment changes the definition of a cybersecurity incident. Under Section 500.17, a cybersecurity incident is now defined as an event that has occurred at the Covered Entity, its affiliates, or a third-party service provider that:

1. Impacts the Covered Entity and requires the Covered Entity to notify any government body, self-regulatory agency or any other supervisory body;

2. Has a reasonable likelihood of materially harming any material part of the normal operation(s) of the Covered Entity; or

3. Results in the deployment of ransomware within a material part of the Covered Entity's information systems.

Notification of Cybersecurity Incident

While Covered Entities were already required to notify the Superintendent of Financial Services electronically through the DFS Portal of a cybersecurity incident as promptly as possible, but in no event later than 72 hours after determining that a cybersecurity incident has occurred, the Amendment now requires Covered Entities to provide this notice if the cybersecurity incident occurred at the Covered Entity, its affiliates, or a third-party service provider. Thus, if a breach occurs at an insurance carrier or other third-party administrator or vendor, and such breach would be considered a cybersecurity incident, agents, producers and brokers must now notify DFS. This is true even if the third-party service provider is also providing notice to DFS. Covered Entities must also promptly provide DFS with any information requested regarding the incident and update DFS with material changes or new information previously unavailable.

Notification of Extortion Payment

DFS continues to discourage making extortion payments. Under the Amendment, Covered Entities must:

a. Notify DFS within 24 hours of any extortion payment made; and

b. Within 30 days of a payment, provide DFS with a written description of the reasons payment was necessary, alternatives to payment considered, diligence performed to find alternatives to payment and to ensure compliance with applicable regulations, including those of the Office of Foreign Assets Control.

Certification of Compliance

In addition to notifying DFS of the above, beginning April 15, 2024, every year Covered Entities must electronically submit a certification of material compliance with Part 500 or acknowledgment of noncompliance to DFS. If the Covered Entity did not comply, its written acknowledgment must:

This document is designed to highlight various employee benefit matters of general interest to our readers. It is not intended to interpret laws or regulations, or to address specific client situations. You should not act or rely on any information contained herein without seeking the advice of an attorney or tax professional. © Emerson Rogers, LLC. All Rights Reserved.
CA Insurance License #0C94240.

a. Acknowledge that, for the prior calendar year, the Covered Entity did not materially comply with all the requirements of Part 500;

b. Identify all sections of the Cybersecurity Regulation that the Covered Entity has not materially complied with and describe the nature and extent of such noncompliance; and

c. Provide a remediation timeline or confirmation that remediation has been completed.

The Covered Entity's certification of compliance or acknowledgment of noncompliance must be submitted electronically in the form set forth on the department's website and must be signed by the Covered Entity's highest ranking executive and its Chief Information Security Officer ("CISO"). If the Covered Entity does not have a CISO, the certification or acknowledgment must be signed by the highest-ranking executive and by the senior officer responsible for the cybersecurity program of the Covered Entity.

Action

All Covered Entities, which include agents, producers and brokers, should review the Amendment and evaluate their obligations under all applicable laws. In the event a Covered Entity determines a cybersecurity incident has occurred at the Covered Entity, its affiliate, or at a third-party service provider, such as an insurance carrier, third-party administrator or other vendor, or is notified of same, the Covered Entity must report same to DFS within 72 hours. Each Covered Entity must provide a certification of material compliance or acknowledgment of noncompliance to DFS before April 15, 2024.

Resources

NYS DFS Cybersecurity Resource Center:
https://www.dfs.ny.gov/industry_guidance/cybersecurity

For a copy of the Amendment:
https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf

DFS Portal:
https://myportal.dfs.ny.gov/

Instructions for Reporting A Cybersecurity Incident:
https://www.dfs.ny.gov/system/files/documents/2023/11/reporting-cybersecurity-incidents.pdf

Instructions for Reporting an Extortion Payment:
https://www.dfs.ny.gov/system/files/documents/2023/11/instruct_reporting_extortion_payments.pdf

This document is designed to highlight various employee benefit matters of general interest to our readers. It is not intended to interpret laws or regulations, or to address specific client situations. You should not act or rely on any information contained herein without seeking the advice of an attorney or tax professional. © Emerson Rogers, LLC. All Rights Reserved.
CA Insurance License #0C94240.