REPORTING GUIDE

New York State Department of Financial Services (NYS DFS): Filing a Cybersecurity Incident Report for Covered Entities

StratisAdvisory

RISK | STRATEGY | CYBER COMPLIANCE MANAGEMENT

NYS DFS Cybersecurity Incident Reporting Guide

Under New York's Cybersecurity Regulation 23 NYCRR Part 500, the New York State Department of Financial Services (NYS DFS), must be notified by a Covered Entity about the occurrence of a cybersecurity event, which is defined as *"any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse an information system or information stored on such information system."*

Who needs to submit a Cybersecurity Incident?

All NYS DFS Covered Entities or any person required to operate under a license, registration, charter or similar authorization under the Banking, Insurance or Financial Services Law of the State of New York.

When should a Cybersecurity Incident be reported?

A notification must be filed as soon as possible and no later than 72 hours upon determination that a cybersecurity incident occurred within the Covered Entity, at its Affiliates or Third-Party Service Providers.

What are the considerations when filing a Cybersecurity Incident Report?

The Cybersecurity Incident must be reported when:

- *It impacts the Covered Entity and requires the Covered Entity to notify any government or supervisory body, or a self-regulatory agency;*
- *There is a reasonable likelihood of significantly harming any crucial part of the Covered Entity's normal operations; or*
- *The incident warrants the deployment of ransomware within a substantial scope of the Covered Entity's information system, especially when there is an impact to non-public information or the multi-factor authentication system.*

What information is included in the Cybersecurity Incident Report?

Apart from the Covered Entity's corporate information, the following must be included in the Report:

- *Contact person's name, as well as title, address, phone number and email address,*
- *Notification date and name of filer,*
- *Date/s of the cybersecurity incident/s,*
- *Where the cybersecurity event occurred, whether the covered entity or the vendor or service provider, and*
- *Description of the cybersecurity incident/s and its impact to the filing entity (Filing Institution).*

How is the Cybersecurity Incident Report filed?

The Cybersecurity Incident is electronically filed through the NYS DFS Portal: https://myportal.dfs.ny.gov/. An account must be created and signed into to access the filing system.

The Portal also requires the filer to use an identifying number (e.g. a NYS License number, NAIC/NY Entity number, NMLS number, Institution number, etc.) to ensure that reports match to the correct entity or individual. NYS DFS also provides step-by-step instructions here.

Reporting Tips

- *Once the Cybersecurity Incident is filed, a confirmation will appear in the portal that contains a receipt number, entity ID number, date of notice, name of filer and the date/s of the cybersecurity incident/s, which should be kept for documentation purposes. Similarly, an email confirmation will also be sent to the submitter.*
- *NYS DFS recommends against paying ransoms. However, covered entities are not prohibited in making such payments in the event of a ransomware attack. If such extortion payment was made, a Notice of Extortion Payment must be filed within 24 hours of payment. Additional information on reporting an extortion payment can be found here.*
- *Review insurance policies to determine to what extent the incident may be covered, inclusive of costs related to retaining any digital forensic and incident response companies.*
- *Review FinCEN Advisory FIN-2021-A004 on whether the incident requires the filing of a Suspicious Activity Report (SAR).*

For more information, you can visit the how to Report a Cybersecurity Incident page found in NYS DFS' Cybersecurity Resource Center.