

CYBERSECURITY AND DATA PRIVACY INFORMATION MEMO

MAY 12, 2021

New York State Department of Financial Services Announces Two Cybersecurity Settlements

The Cybersecurity Division of the New York State Department of Financial Services (DFS) continues to ramp up enforcement of the Cybersecurity Regulation. In two recent settlements, DFS has begun to offer insight into how it intends to enforce the Cybersecurity Regulation, [23 NYCRR Part 500](#). We previously covered the Cybersecurity Regulation [here](#).

In both cases, DFS focused on failures by the regulated entities to report cyber breaches in a timely manner as required by the Cybersecurity Regulation. Both matters also involved breaches of company email systems and failure to adequately control access to systems containing sensitive personal customer data. As discussed below, these settlements highlight three core requirements of the Cybersecurity Regulation: timely reporting of breaches ([23 NYCRR 500.17](#)); implementation of a cybersecurity risk assessment ([23 NYCRR 500.9](#)); and implementation of adequate access controls, including multi-factor authentication ([23 NYCRR 500.12](#)).

On March 3, 2021, DFS announced a settlement with Residential Mortgage Services, Inc. (RMS), a licensed mortgage banker. As part of the settlement, RMS agreed to pay a \$1.5 million penalty and implement improvements to its cybersecurity program to ensure compliance with the Cybersecurity Regulation. According to the agency, a DFS examination in July 2020 uncovered evidence that RMS had been the subject of a cyber breach in 2019 which had not been reported to DFS, in violation of Part 500.17 of the Cybersecurity Regulation. The breach involved a phishing email sent to the email account of an RMS employee with access to sensitive customer data. The employee responded to the phishing email by following a link to a malicious website where the employee provided her login credentials to the intruder. In its examination of RMS, DFS determined that RMS violated the Cybersecurity Regulation by failing to report the breach. DFS also determined that RMS also violated the regulation by failing to have in place a comprehensive cybersecurity risk assessment.

On April 14, 2021, DFS announced a settlement with National Securities Corporation (National Securities), a licensed insurance company. National Securities agreed to pay a \$3 million penalty in connection with the settlement. DFS's investigation of National Securities uncovered evidence that National Securities had been the subject of four cyber breaches between in 2018 and 2020, two of which had not been reported to DFS as required by the Cybersecurity Regulation. The breaches involved unauthorized access to the email accounts of National Securities employees and independent contractors. Among other things, DFS found that National Securities violated the Cybersecurity Regulation by failing to implement multi-factor authentication, or reasonably equivalent access controls.

How Can We Help?

Please contact [John D. Clopper](#) or any [attorney](#) in our [Cybersecurity and Data Privacy practice](#) if we can help your business determine the applicability of the DFS Regulations to your business, assist with any interpretation of the DFS Regulations as they apply to your business, or assist with identification of actions that must be taken with respect to your third-party service providers.

