LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

NY, FTC Dial Up Heat With Financial Data Security Upgrades

By **Allison Grande**

Law360 (November 9, 2023, 9:33 PM EST) -- New York's financial services regulator and the Federal Trade Commission have recently moved to beef up rules governing data breach disclosures and the protection of financial data, creating new risks for financial institutions and their executives and adding fuel to broader efforts to expand cybersecurity regulations in this area.

The New York State Department of Financial Services announced Nov. 1 that it has amended its cybersecurity regulations to enhance cyber governance and reporting obligations, including by establishing requirements for senior leadership at banks, insurers and other covered entities to take a more active role in cybersecurity efforts and for those entities to report ransomware payments to the regulator.

The changes came on the heels of the FTC disclosing late last month that it has tweaked its Safeguards Rule under the Gramm-Leach Bliley Act to require nonbank financial institutions such as mortgage brokers, motor vehicle dealers and payday lenders to report data breaches and other security events to the agency.

The updates share the common themes of increasing the pace and transparency of data breach disclosures while emphasizing the importance of preparedness to improve the cybersecurity posture of companies across the financial services sector, experts told Law360.

"We can see with these amendments a consolidation in the approach that regulators are taking to address these cybersecurity risks," said Craig Hoffman, co-leader of the cybersecurity practice at BakerHostetler. "They're expecting a more mature cyber program to be built up and for organizations to have updated data breach risk assessments, and there's a strong push to have executive management be more involved in the oversight of the program."

The changes carry significant liability risks for both organizations and their executives, especially in light of the appetite that the FTC and NYDFS have shown in the past to aggressively police these issues.

The FTC has repeatedly come down hard on companies that allegedly fail to adequately protect sensitive information such as financial, health and children's data. That push includes enforcement actions accusing companies such as online tax preparation service TaxSlayer and mortgage analytics firm Ascension of violating their responsibilities under the Safeguards Rule to develop, implement and maintain a comprehensive information security program and ensure third-party vendors are capable of similarly protecting data.

New York's financial services regulator has also been an active enforcer since finalizing its first-of-their-kind cybersecurity rules in 2017. The department targeted a data leak at insurer First American for its first enforcement action under the regulation in 2020. And it has kept up the pressure with moves such as hitting mortgage servicer OneMain Financial Group LLC with a $4.25 million penalty in May for "significantly increasing" its vulnerability to cybersecurity events by failing to effectively manage third-party service provider risk and manage access privileges.

"The department has made cybersecurity enforcement a priority in recent years, and the amendments signal that the department will continue to regard this as a priority," said Justin Herring, a Mayer Brown LLP partner and former executive deputy superintendent of the cybersecurity division at NYDFS. He added that similar moves by regulators such as the FTC and U.S. Securities and Exchange Commission illustrate that the department "won't be alone" in stepping up enforcement in the financial arena.

Given this climate, it's vital for covered organizations to pay attention to and implement the recent changes, experts say.

With respect to the updated NYDFS rules, its trailblazing work in this space is likely to prompt "clients across the country and across industries" to keep an eye on what the regulator is doing and use the standards as a benchmark for their own programs "even if they themselves are not directly regulated" by the department, noted Micaela McMurrough, co-chair of the global and multi-disciplinary technology group at Covington & Burling LLP.

The updated cybersecurity regulations create a new "Class A" company category that imposes heightened obligations on organizations that have more than 2,000 employees or have made more than $1 billion in gross annual revenue in each of the last two fiscal years.

"The regulation never took a 'one size fits all' approach, but rather was rooted in a risk-based assessment," McMurrough noted. "At the same time, the recognition that there are higher expectations for larger entities is an important one."

The revamped rules also add a list of factors that the regulator may consider for enforcement purposes, a move that "is truly ground-breaking in that it recognizes that cyber incidents will occur, and allows the regulator to consider not just how the incident occurred but how the entity behaved in the wake of the incident when making enforcement decisions," according to McMurrough.

In parsing the updated NYDFS rules, which attorneys noted are more comprehensive and proscriptive than the FTC amendments, covered organizations will confront not only "quite a bit of expansion of existing regulations," but also "some substantial new governance and reporting requirements that aren't in the original regulation," noted Herring of Mayer Brown.

"These requirements will prove almost impossible to comply with during an incident if companies do not already have detailed response plans in place," Herring added.

A major change that organizations will soon need to grapple with is the heightened obligations for their senior governing body to have "sufficient understanding of cybersecurity-related matters" and to confirm that the covered entity has "sufficient resources to implement and maintain an effective cybersecurity program."

"NYDFS has always taken what they consider a risk-based approach to its cybersecurity rule, allowing covered entities to develop their cyber programs based on their unique cyber profile," said Elise Elam, a cybersecurity attorney at BakerHostetler. "While that's still the case under this amended rule, the department has made it clear that it expects senior leadership to take a bigger role and make sure they have buy-in with their cybersecurity programs."

These bolstered requirements include having both an organization's highest-ranking executive and its chief information security officer sign the certification of material compliance that's due every April 15 and, beginning April 29, ensuring that cybersecurity policies are annually reviewed and approved by the senior governing body or senior officers.

Additionally, as of Nov. 1, 2024, the CISO will need to timely report to senior executives on "material cybersecurity issues, such as significant cybersecurity events and significant changes to the cybersecurity program," and the senior governing body must be able to "exercise oversight" of its cybersecurity risk management.

"For those facing these requirements, it creates a challenging dynamic and puts added pressure on them to be well-prepared," said Jordan Rae Kelly, head of cybersecurity for the Americas at FTI Consulting. "There's no longer going to be an acceptance of the belief that cybersecurity is hard to understand so it should just be left to the CISO."

Financial services executives have already started taking some of these steps, with Jamie Singer, a managing director in the cybersecurity and data privacy communications practice at FTI Consulting, noting that she's seen an uptick in board participation in table-top exercises that simulate the company's response to a data breach and similar preparation activities.

"There's absolutely a growing appetite for the board to be involved," Singer said. "But a challenge is determining how involved and active they need to be in breach responses and other activities."

With the NYDFS making it clear that it expects robust board involvement on the cybersecurity front, executives and other senior leadership need to think carefully about what role they're playing and what that means for their potential exposure to liability.

These considerations are particularly important in light of the SEC's recent move to sue not only SolarWinds but also its CISO over misleading disclosures related to a sprawling 2020 cyberattack.

The push by the commission — which also took the step earlier this year of revamping its own cyber disclosure regulations to require companies to publicly report significant data breaches — to hold an executive liable for allegedly engaging "in a campaign to paint a false picture of the company's cyber controls environment" highlights the enhanced risk financial executives are likely to have in light of the expanded responsibilities under the NYDFS rules, Mayer Brown's Herring noted.

While the actions aren't related, the fact that the SEC's SolarWinds lawsuit came during the same week as the finalization of the regulation that the highest ranking executive needs to sign off on cybersecurity compliance "certainly heightens awareness of these risks for companies," Herring said. He added that this emphasis on the board's role in cybersecurity risk management is part of a growing trend of regulators expecting more out of a board on a range of issues, including artificial intelligence and climate change.

Under the amended NYDFS regulations, covered financial institutions and their leadership will also have to contend with a fast-approaching deadline to tighten their disclosures related to ransomware attacks, attorneys noted.

Beginning Dec. 1, organizations will need to report any ransomware payment they make to unlock systems and recover data in connection with a cyberattack within 24 hours of payment and, within 30 days from that, provide additional information to the regulator about the reason the payment was necessary, alternatives that were considered, and the research and diligence it conducted to find alternatives.

While the regulation already requires financial institutions to report breaches to the department within 72 hours of determining a breach has occurred, these expanded notification requirements related to increasingly prevalent ransomware attacks will require companies to rethink how they approach response decisions that they could previously keep largely quiet from regulators.

"The idea of paying a ransom is a polarizing topic, and financial institutions are going to have to be able to explain their decision-making," Singer of FTI Consulting said.

Given that the details, particularly in the immediate aftermath of a ransomware attack, are so "fluid," fulfilling this obligation will require organizations to balance how to "communicate relevant facts and information without speculating one way or another," Singer added.

The new ransomware disclosure obligations also highlight "how complex incident response obligations have become" for businesses, which have to consider 50 state breach notification laws and myriad federal and international regulations when responding to a data security incident, noted Mayer Brown's Herring.

"In 2017, when the NYDFS regulations first came out, the department stood largely apart," Herring said. "But the world has changed a lot, and it's going to be almost impossible for companies to get all these overlapping reporting rules right unless they do a fair amount of work in the incident planning stage to figure out who's responsible for doing what during a high-pressure, fast-moving cyber event."

The FTC introduced yet another breach reporting obligation with its latest update to the Safeguards Rule, which will require nonbank financial institutions such as mortgage brokers, motor vehicle dealers and payday lenders to report data breaches involving the unauthorized acquisition of information of at least 500 people to the agency as soon as possible, and no later than 30 days after discovery.

The notice to the FTC must include certain information about the event, such as the number of consumers affected or potentially affected.

While nonbanking financial institutions are already obligated under the Safeguards Rule to develop and maintain comprehensive security programs to keep consumers' information safe, this expanded reporting obligation is likely to be a challenge, particularly for smaller businesses that haven't had to construct such breach response programs before and will need to allocate additional time and resources to compliance, attorneys noted.

"The FTC made clear that one primary reason for adopting these new breach notification requirements is so the FTC could monitor emerging data security threats affecting nonbanking financial institutions

and facilitate prompt investigations following major security breaches," noted Amy Mushahwar, a partner on Alston & Bird LLP's privacy, cyber and data security team.

The FTC's plan to make its notification information available to the public could also present additional challenges by "adding even more pressure for companies during the intense press cycle that occurs during a data breach notification," Mushahwar added.

"The press cycle often readily includes class action recruitment websites from the moment a breach is public, without a true understanding if there is, or will be, any actual harm," Mushahwar said. "If this notification information must be updated, which can occur especially if breach event data must be analyzed in waves, it might even create several press cycles that could snowball. "

The expanded FTC rule will take effect 180 days after the upcoming publication of the final regulation in the Federal Register, according to the commission.

While this timeline is longer than covered financial institutions have to get into step with the NYDFS ransomware reporting rules, compliance with the department's rules will be a more lengthy process, given that the regulation goes into force in stages over the next two years, attorneys noted.

Some of the final obligations are to be able to conduct regular automated scans of systems to discover vulnerabilities and put in place enhanced user access privileges and controls to protect against malicious code beginning in May 2025, and to implement multi-factor authentication for all individuals accessing information systems and compile a detailed asset inventory starting in November 2025.

While this may sound like a long lead-in time, some of these requirements "could require new technology like updating systems to accommodate controls, and two years is not a lot of time for IT upgrade projects," Mayer Brown's Herring noted.

The financial regulator has also said it plans to host a series of webinars and issue guidance to provide additional details about the amended regulations, which could provide companies with important clarity on lingering questions about which top executives are specifically on the hook for certifications and what details need to go into ransomware reports.

As these developments play out, companies should ensure they're setting up the processes and procedures relevant to their companies' size and risk profile to get into step with their range of new obligations, attorneys say.

"If a company can demonstrate that their method is correct but if things go wrong because implementation is challenging, there's likely to be a level of understanding that the organization was trying to do things the right way," BakerHostetler's Hoffman said. "If you have a cybersecurity incident that exposes an underlying area of noncompliance, that's often what puts companies in regulators' crosshairs."

Given these risks, BakerHostetler's Elam advised, "To the extent that they don't already, covered entities definitely need to get a plan in place and start following it now, because NYDFS is taking this seriously."

--Additional reporting by Katryna Perera and Hailey Konnath. Editing by Kelly Duncan and Emily Kokoll.