Insights, News & Events

WHAT A $2.25M NY CYBERSECURITY SETTLEMENT MEANS FOR BUSINESSES: YOUR 4-STEP ACTION PLAN

Insights
Jun 10, 2026

What a $2.25M NY Cybersecurity Settlement Means for Businesses: Your 4-Step Action Plan

A recent $2.25 million settlement between an insurance company and the state of New York presents a cautionary tale for businesses in the Empire State. The New York State Department of Financial Services (NYDFS) found that the company's incident response plan was inadequate and allowed threat actors to access New Yorkers' personal information. Settlements between state cyber regulators and impacted organizations are often the result of the organizations' missteps following a breach. In this case, NYDFS not only found that the company failed to meet reporting requirements following a cyber incident, but also that its preventative measures were deficient. Here's why that's important and what your organization should do to avoid similar sanctions.

The Significance of the Settlement

The insurance company agreed to settle the state's claims after an NYDFS investigation concluded that the insurance company's preventative cybersecurity policies and practices that were in place before the breach failed to satisfy the state's regulatory threshold. The state also found that the company failed to report the breach to officials in a timely manner. NY's Cybersecurity Regulation requires covered entities to notify regulators of a cybersecurity incident

Related People

Logan S. Booth, CIPP/US
Of Counsel

720.644.2889

Kate Dedenbach, CIPP/US
Of Counsel

248.901.0301

"promptly" and no later than 72 hours after a determination that a reportable event has occurred.

Specifically, the state said the insurance company's cybersecurity posture did not meet requirements related to retention settings, controls, procedures, and policies that exist to protect the information systems and consumer data of regulated financial institutions, according to the April 30 settlement.

Key issues identified by investigators:

- No set policies or procedures for the periodic and secure disposal of non-public information that is no longer necessary for business operations or for other legitimate business purposes.
- No written or implemented policy addressing incident response.
- Didn't maintain an incident response plan that sufficiently addressed their reporting obligations to regulators.

The NYDFS acknowledged that the company cooperated throughout the investigation, promptly investigated the cybersecurity event, and continued to resolve the issues identified.

What This Means for Your Organization

As cyber incidents become more common, regulators are focusing on organizations that handle personal information. The growing expectation is that entities will implement best practices and adhere to regulatory guidance before attacks happen. The settlement secured by NYDFS is one example showing that policymakers are becoming more aggressive in enforcement when minimum requirements don't appear to be met.

The Key Lesson: Multi-state businesses or companies operating in New York should maintain a written cybersecurity response plan that includes details about how to report the incident to regulators. Work with your data management team to ensure your company isn't retaining non-public or sensitive information if it's no longer needed for your business. Consult with privacy counsel if you need assistance crafting a response plan

Daniel Pepper, CIPP/US

Partner

303.218.3661

Service Focus

Privacy and Cyber

Industry Focus

Healthcare

Related Offices

New York

or identifying potential compliance pitfalls within your data management infrastructure.

Your 4-Step Action Plan

To help insulate your organization from potential cybersecurity compliance headaches, consider taking these four steps:

1. Audit Your Incident Response Plan (IRP): Many organizations have IRPs, but they're static documents that are only as current as the date of their most recent publication. Data protection and cybersecurity regulations are constantly evolving, and it's important that your IRP reflects that. Frequent (annual) reviews and audits of your incident response plans are recommended. Be sure to consult with external advisors who are aware of the most current guidance and can review your plans for compliance.

2. Communicate with Regulators: When zero-day vulnerabilities are identified by vendors, they sometimes alert regulators. Regulators will often communicate this information to entities under their jurisdiction that are likely to use the vendors' products, as was the case in this investigation and settlement. Having open channels of communication and maintaining good working relationships with cyber regulators makes it more likely that you'll receive useful instructions and guidance.

3. Track Regulatory Developments: The regulation at issue in this settlement became effective in March 2017 and was amended in November 2023. As new rules are implemented at a rapid pace, it can be difficult for in-house CISOs and GCs to keep up with changes, especially if your organization operates in multiple jurisdictions. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information directly to your inbox.

4. Adhere to Reporting Requirements: Addressing and mitigating a breach is intense work. The regulatory notification clock can run out before you may realize, which can support fines even without intent to delay or conceal. Retaining counsel early adds bandwidth and shifts this work to a team that handles these issues routinely.

Conclusion

If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Fisher Phillips Data Privacy and Cybersecurity Practice Group. Fisher Phillips will continue to monitor developments and provide updates as warranted. And again, sign up for alerts from Fisher Phillips' Insight System to stay on top of information that could impact your business.