REQUEST FOR COMMENT ON REVISED PROPOSED SECOND AMENDMENT TO 23 NYCRR Part 500

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

August 14, 2023

I. INTRODUCTION

In response to New York's Department of Financial Services ("DFS") Revised Proposed Second Amendment to 23 NYCRR Part 500, Cybersecurity Requirements For Financial Services Companies ("proposed amendment") CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

We appreciate the DFS's continued engagement with stakeholders and the opportunity to provide comments on the updated proposed amendment. Notably, the DFS also released a document titled *Assessment of Public Comments on the Proposed Second Amendment to 23 NYCRR 500* ("assessment of public comments"); this document reflects considerable effort to capture stakeholders' input and provide insight into the DFS's views of previous comments.

CrowdStrike supports the amendment's goal of better protecting New York's and the nation's financial services sector from cybersecurity threats. These threats continue to evolve and grow more severe. In a recent report, for example, we found that interactive intrusion activity against the financial services industry increased by over 80% over the

past year.[1] Furthermore, the report found a 147% increase in access broker[2] advertisements on the dark web, a 95% rise in cloud attacks, and a sharp increase in credential theft – making steps to enhance cybersecurity in the sector timely and appropriate.

CrowdStrike previously commented on the initial version of the proposed amendment, and we've reemphasized certain points in this response.[3] While we do not have feedback on every aspect of the proposed amendment, we do want to offer several points that may be of value to the DFS as it considers the proposed rule.

A. Cybersecurity Risk Management Practices

We commend the DFS for strengthening cybersecurity by amplifying attention given to this issue and defining expectations. There are some key steps organizations should take to strengthen their security posture. The proposed amendment includes many of today's most effective cybersecurity practices. Notably, several of these practices are also mandated in the May 2021 federal Executive Order (EO) 14028 on Improving the Nation's Cybersecurity.[4]

CrowdStrike applauds the continued inclusion of endpoint detection and response (EDR), identity protection and authentication, and logging practices and principles in the proposed amendment. We recommend they continue to be included in the final amendment. In our experience, organizations that do not leverage these practices are not set up for success against cyber attacks.

In our previous comments, we also suggested the consideration of threat hunting, machine learning-based prevention, zero trust, and managed service providers principles and technologies. We view these as best practices for a comprehensive, risk-based, cybersecurity strategy. In the assessment of public comments, the DFS states, "*The use of machine- learning-based prevention and zero-trust architecture are*

[1] 2023 *Threat Hunting Report*, CrowdStrike, https://www.crowdstrike.com/resources/reports/threat-hunting-report/.
[2] Access Brokers: Who Are the Targets, and What Are They Worth?, https://www.crowdstrike.com/blog/access-brokers-targets-and-worth/
[3] *Request for Comment on Proposed 2nd Amendment to 23 NYCRR Part 500*, CrowdStrike, Jan 9, 2023. https://www.crowdstrike.com/wp-content/uploads/2023/02/New-York-Cyber-Amendment-Comments.pdf.
[4] White House, *Executive Order 14028: Improving the Nation's Cybersecurity* (May 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

also appropriate measures that companies may take to protect their systems. However, the Department declines to mandate these methodologies at this time to avoid becoming overly prescriptive, especially given the many different sizes and types of entities that the Department regulates." The assessment of public comments also references threat hunting and managed service providers, and uses the same explanation for why they are not included in the updated proposed amendments.

CrowdStrike respects, and agrees with, the concept that different entities require different cybersecurity solutions. However, as stated previously, we view threat hunting, machine learning-based prevention, zero trust, and managed service providers principles and technologies as emerging best practices within a comprehensive cybersecurity strategy. Therefore, we would suggest the DFS add a section of "recommended" additional cybersecurity steps and include threat hunting, machine learning-based prevention, zero trust, and the use of managed security service providers. By listing these additional cybersecurity best practices, the DFS would provide a useful reference point for a mature security program.

Finally, the proposed amendment adds additional MFA requirements to further protect entities from identity and credential theft attacks.[5] As the proposed amendment recognizes, due to fundamental problems with today's widely-used authentication architectures, organizations must incorporate new security protections focused on authentication. Importantly, Zero Trust architecture and identity threat protection concepts are important adjuncts to MFA-based guidance because they radically reduce or prevent lateral movement and privilege escalation during a compromise, and can stop attacks even if legitimate credentials are compromised and MFA is bypassed.

B. Reporting Harmonization

As the DFS reviews this proposed amendment, and drafts other pieces of regulation, CrowdStrike urges alignment where possible with existing rules and regulations. The proposed amendment has the opportunity to strengthen cybersecurity for organizations that play critical roles in the everyday lives of many Americans as well as the economy writ large. Nonetheless, new regulation will not be issued in a vacuum but instead amongst a venn diagram of cybersecurity regulations. We recommend alignment with the Cyber Incident Reporting for Critical Infrastructure Act of 2022

[5] CrowdStrike supports protecting against identity and credential theft attacks, given that our new 2023 *Threat Hunting Report* found that 62% of interactive intrusions involved compromised identities and observed a 583% increase in a growing identity-based attack technique called "Kerberoasting".

("CIRCIA") and the forthcoming implementing regulation. Additionally, there will be harmonization recommendations resulting from the ongoing work of the Cyber Incident Reporting Council to align federal cyber incident structures and requirements, that should be followed when appropriate by state governments.

However, in the assessment of proposed comments, the DFS states "*the Department believes that the definition of "cybersecurity incident" used in CIRCIA is too narrow because it would not include many of the successful cybersecurity events that occur at covered entities. The Department has endeavored to harmonize and align where appropriate and practical and believes that any differences are necessary to further the purpose of the amendment.*" CrowdStrike urges the DFS to reconsider this stance and align their definition of cybersecurity incident with CIRCIA's forthcoming definition and narrow the definition to not include attempted attacks.

We recommend the DFS, and any government body requiring reporting, endeavor to achieve balance in scoping reportable incidents. The volume of resulting incident reports should be sufficient to discover and alert entities about systemic and/or widespread incidents. But the volume should not be so great as to create "noise" for analysts and additional reporting burdens for threat activity that is prevented and remediated prior to a material impact.

In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and regulations. In most cases, organizations using contemporary cybersecurity solutions are alerted to malicious activity occurring in their environment. The nature of these alerts may vary, and could cover something like the installation of malicious software on one system, or the compromise of a single account. In scenarios where defenders see these alerts and address them quickly, the alert may not rise to the threshold of a cybersecurity "incident," particularly where the threat actor has not meaningfully achieved their objective, accessed sensitive information, and the like.

III. CONCLUSION

The DFS's proposed amendment represents a thoughtful attempt to strengthen security outcomes in a complex legal and policy environment. Generally speaking, the financial sector uses strong cybersecurity practices due to the amount of sensitive data they protect and the regulations to which they are subject. With an emphasis on adoption of practical security practices, these new requirements can raise the already

high standard of cybersecurity in the financial sector. As the DFS moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any proposed legislative updates focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with one of the world's most advanced cloud-native platforms for protecting critical areas of enterprise risk – endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Learn more: https://www.crowdstrike.com/.

V. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Elizabeth Guillot
Manager, Public Policy

Email: policy@crowdstrike.com

©2023 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are trademarks owned by CrowdStrike, Inc. and

registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

***