CROWDSTRIKE

REQUEST FOR COMMENT RESPONSE

Federal Communications Commission: Data Breach Reporting Requirements

WC Docket No. 22-21

February 22, 2023

I. INTRODUCTION

In response to the Federal Communications Commission's (FCC) Notice of Proposed Rulemaking ("NPRM") on data breach reporting requirements, 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

The legal and regulatory environment surrounding mandatory data breach reporting is complex, due in no small part to the overlapping and duplicative reporting obligations that organizations face. Organizations that regulators consider to be critical infrastructure face particular complexity. However, data breach reporting requirements that have an appropriate threshold for reporting, timeline, and alignment with other reporting schemes, can help incentivize organizations, including government agencies, to adopt best-in-class cybersecurity practices.

While we do not have feedback on every aspect of the NPRM, we offer feedback on several points that may be of value to the FCC as it continues the rulemaking process.

A. Definitions & Criteria

Breach. The FCC proposes expanding the current definition of breach to "any instance in which a person, without authorization or exceeding authorization, has gained access to, used, or disclosed Customer Proprietary Network Information (CPNI)." CrowdStrike

believes this definition is too broad and will result in an abundance of unactionable reports. As the FCC continues to draft its definition of breach, we recommend considering the following distinctions to narrow the scope of the definition of "breach."

Alerts versus Incidents. In cybersecurity, an important distinction exists between alerts and incidents, which should help inform notification scenarios and standards. In most cases, carriers using contemporary cybersecurity solutions should be 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 most scenarios where defenders see these alerts and address them quickly, an issue does not meet any reasonable standard of a cybersecurity "incident" because the threat actor has not meaningfully achieved their objective or accessed sensitive information. With this in mind, an alert from a third-party cybersecurity provider should not be included in the definition of "breach."

Impact versus Serious Impact. Another important distinction that merits discussion is that of impacts versus serious impacts. Not all breaches have the same level of severity. For example, an incident where a threat actor sees a list of user names might have a small or negligible impact on affected parties. Whereas, another incident in which a threat actor exfiltrates complete financial or medical records may have a severe impact. Consideration of the impact and severity of a breach is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation measures. CrowdStrike recommends that only breaches that have serious impact fall under the reporting scope.

Mitigated Attacks. Threat actors may choose to target an organization in a series of steps, rather than in a single attack. In fact, an initial intrusion into an enterprise is often not a threat actor's end goal. Instead, threat actors may first deploy a backdoor, harvest credentials, or use other methods in order to move laterally throughout a network and to their ultimate objective. A threat actor may be stopped at any of the steps in the killchain, and this raises important questions that impact the breach notification process - namely, if a breach is mitigated, does the obligation to notify still exist? For example, if a threat actor enters an enterprise with the goal of exfiltrating data but is stopped before the infiltration occurs, the possible resulting impact of the incident has been mitigated. In such an example, it is a breach when the threat actor enters the network but it could have been a substantial breach if the goal of data exfiltration was reached. Ultimately, this means that a data breach in and of itself may not pose a risk of harm to consumers where

successful steps have been taken to mitigate the breach and prevent exfiltration. Mitigated breaches should not be included in the reporting scope.

Harm. The FCC should adopt a harm-based trigger as part of its breach notification reporting requirement and only require breaches that cause serious harm to be reported. We acknowledge that adopting such a trigger may result in a regulatory overlap with the Federal Trade Commission (FTC), as well as other agencies and we address this point below.

In defining what constitutes a reportable level of harm, it is critical to focus on internationally-accepted principles-based concepts rather than prescriptive technical requirements. The FCC should adopt a risk-based approach and take the following factors into consideration:

- Nature of the data in question: Is the data in question sensitive? Is the data solely CPNI? Does the data include CPNI and other personal data elements?
- Impact of a breach: Was the data successfully exfiltrated?
- Mitigations: Did the carrier successfully mitigate impacts?

B. Breach Notification Reporting Requirements

Proposed Reporting Timeline. The FCC proposes amending the current reporting timeline to law enforcement from "no later than 7 business days after a reasonable determination of a breach" to "as soon as practicable after discovery of a breach," as well as amending the reporting timeline to customers to "without unreasonable delay after discovery of breach…" The FCC also asks, in the context of adding a harm-based trigger to reporting obligations, whether there should be a rebuttable presumption of harm to consumers, thereby necessitating disclosure of the breach to customers.

We recommend that any reporting timeline requirements be considered in context. Not all cyber incidents have the same level of severity and rise to a level of individual harm that necessitates reporting. For example, an incident where a threat actor gains access to a single resource, is unable to escalate privileges or move laterally, cannot interact with sensitive data, and is quickly ejected from the environment due to strong security practices likely would have a minor impact on the covered entity. Whereas, another incident in which a threat actor infiltrates, moves laterally, and is able to control OT systems may have a severe impact. While these are important distinctions, the two incidents could look similar in the early investigation stage.

Consideration of the impact and severity of an incident is important not only when initially assessing evidence of an intrusion but also in discerning the efficacy of mitigation

measures. Furthermore, exacerbating factors where public notice could be detrimental to an ongoing incident response investigation include, for example, when data extortion is at play, a law enforcement investigation mandating confidentiality, or where it may take additional time to incorporate measures necessary to prevent an even more significant impact (such as in vulnerability disclosure).

Consequently, we caution against creating a rebuttable presumption of harm that would necessitate disclosure to customers and we encourage the FCC to consider developing guidance as part of the NPRM on what "as soon as practicable" and "without unreasonable delay" mean. Any timelines articulated should be no shorter in duration than the 72 hour window outlined in the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA")[1] which was signed into law in March 2022.

FCC's Role Relative to Other Agencies & Overlapping Reporting Requirements. As recognized in the NPRM, mandatory breach notification reporting requirements is an extensive area of regulation and as a result, organizations often face duplicative reporting requirements.

To truly achieve the goal of minimizing duplicative reporting requirements, federal agencies should develop a harmonized approach and establish a one-stop shop for reporting. The FCC should work with other agencies, such as the FTC and Cybersecurity and Infrastructure Security Agency ("CISA"), to have a uniform set of data fields so that organizations with overlapping requirements have a simpler method of disclosure.

We agree with the FCC and encourage submitting reports online. To streamline the reporting process and ease the burden of duplicative reporting obligations, the FCC should explore creating workflows that would allow carriers to explicitly permit the FCC to refer and receive reports from other regulators.

To the extent that a breach of CPNI is the result of a cyber incident and a carrier's notification reporting is covered under CIRCIA, the FCC's reporting requirements should be aligned with what is outlined in CIRCIA. Additionally, we recommend that the FCC consider forthcoming harmonization recommendations resulting from the ongoing work of the Cyber Incident Reporting Council, which was created by CIRCIA to harmonize the many existing federal cyber incident structures and requirements.

III. CONCLUSION

[1] *Cyber Incident Reporting for Critical Infrastructure Act of 2022*: https://www.congress.gov/bill/117th-congress/house-bill/2471/text

Breach reporting is a critical but complex legal and policy area. As the rulemaking process moves forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that a final rule focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

IV. ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about 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

***