UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

Plaintiff, v. CROWDSTRIKE HOLDINGS, INC., GEORGE KURTZ, and BURT W. PODBERE, Defendants.	**CLASS ACTION** **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT FOR VIOLATIONS OF THE FEDERAL SECURITIES LAW

I. INTRODUCTION

Plaintiff individually and on behalf of all others similarly situated, allege the following based upon personal knowledge as to Plaintiff's own acts and upon information and belief as to all other matters based on the investigation conducted by and through counsel, which included, among other things, a review of the public U.S. Securities and Exchange Commission ("SEC") filings of CrowdStrike Holdings, Inc. ("CrowdStrike" or the "Company"), Company press releases, conference call transcripts, investor presentations, analyst and media reports, and other public reports and information regarding the Company. Plaintiff believes that substantial additional evidentiary support exists for the allegations set forth herein, which evidence will be developed after a reasonable opportunity for discovery.

II. NATURE OF THE ACTION

1. This is a federal securities class action on behalf of a class of all persons and entities who purchased or otherwise acquired CrowdStrike Class A common stock between November 29, 2023 and July 29, 2024, inclusive (the "Class Period"), seeking to pursue remedies under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934 (the "Exchange Act"), and SEC Rule 10b-5, promulgated thereunder.

2. CrowdStrike, headquartered in Austin, Texas, is a global cybersecurity company that provides software that helps prevent data breaches. CrowdStrike's customers are major corporations across several industries including airlines, banks, hospitals, and telecommunications providers as well as government entities. CrowdStrike's main product is the Falcon software platform, which purportedly uses artificial intelligence and machine learning technologies to detect, prevent, and respond to security breach threats. The Falcon software is embedded in the computers of CrowdStrike's customers and requires constant updates.

3. Throughout the Class Period, Defendants (defined herein) repeatedly touted the efficacy of the Falcon platform while assuring investors that CrowdStrike's technology was "validated, tested, and certified." This complaint alleges that these statements were false and misleading because Defendants had failed to disclose that: (1) CrowdStrike had instituted deficient controls in its procedure for updating Falcon and was not properly testing updates to Falcon before rolling them out to customers; (2) this inadequate software testing created a substantial risk that an update to Falcon could cause major outages for a significant number of the Company's customers; and (3) such outages could pose, and in fact ultimately created, substantial reputational harm and legal risk to CrowdStrike. As a result of these materially false and misleading statements and omissions, CrowdStrike stock traded at artificially high prices during the Class Period.

4. Beginning on July 19, 2024, investors learned about critical issues with CrowdStrike's technology when a single update pushed by CrowdStrike caused outages for millions of users of Microsoft Windows devices worldwide, including financial institutions, government entities, and corporations (the "CrowdStrike Outage"). Further, CrowdStrike disclosed that the outages had left users vulnerable to potential hacking threats. On this news, shares of CrowdStrike fell ***$38.09***, or ***11%***, to close at $304.96 on July 19, 2024

5. Then, on July 22, 2024, the fallout of the CrowdStrike outage was further revealed as Congress called on Defendant Kurtz to testify regarding the crisis and the Company's stock rating was downgraded by analysts such as Guggenheim and BTIG. On this news, shares of CrowdStrike fell ***$41.05***, or ***13.5%***, to close at $263.91 on July 22, 2024.

6. Investors continued to learn about the legal risk Defendants had concealed on July 29, 2024, as news outlets reported that Delta Air Lines had hired prominent attorney David Boies

to seek damages from the Company following the CrowdStrike Outage. On this news, shares of CrowdStrike fell ***$25.16***, or ***10%***, to close at $233.65 on July 30, 2024.

7. These stock declines following the disclosure of Defendants' fraud caused substantial damages to the Company's investors.

8. Since the CrowdStrike Outage, public commentary from cybersecurity experts has provided evidence that CrowdStrike was taking insufficient precautions regarding such updates, including running insufficient tests.

III. JURISDICTION AND VENUE

9. The claims asserted herein arise under and pursuant to Sections 10(b) and 20(a) of the Exchange Act, 15 U.S.C. §§ 78j(b) and 78t(a), and Rule 10b-5 promulgated thereunder by the SEC, 17 C.F.R. § 240.10b-5.

10. This Court has jurisdiction over the subject matter of this action under 28 U.S.C. § 1331 and Section 27 of the Exchange Act, 15 U.S.C. § 78aa.

11. Venue is proper in this District under Section 27 of the Exchange Act, 15 U.S.C. § 78aa, and 28 U.S.C. § 1391(b), because CrowdStrike is headquartered in this District, and because many of the acts and conduct that constitute the violations of law complained of herein, including the dissemination to the public of materially false and misleading information, occurred in this District.

12. In connection with the acts alleged in this complaint, Defendants, directly or indirectly, used the means and instrumentalities of interstate commerce, including, but not limited to, the mails, interstate telephone communications, and the facilities of the national securities markets.

IV. PARTIES

13. As indicated on the Certification attached herewith, Plaintiff purchased shares of CrowdStrike stock during the Class Period and suffered damages as a result of the violations of the federal securities laws alleged herein.

14. Defendant CrowdStrike is incorporated in Delaware and headquartered in Austin, Texas. CrowdStrike common stock trades on the NASDAQ under the ticker symbol "CRWD."

15. Defendant George Kurtz was the chief executive officer and President of CrowdStrike at all relevant times.

16. Defendant Burt W. Podbere was the chief financial officer of CrowdStrike at all relevant times.

17. Defendants Kurtz and Podbere are collectively referred to as the "Individual Defendants." The Individual Defendants, because of their positions with the Company, possessed the power and authority to control the contents of CrowdStrike's reports to the SEC, press releases, and presentations to securities analysts, money and portfolio managers, and institutional investors, *i.e.*, the market. Each Individual Defendant was provided with copies of the Company's reports alleged herein to be misleading prior to, or shortly after, their issuance and had the ability and opportunity to prevent their issuance or cause them to be corrected. Because of their positions and access to material non-public information available to them, each of the Individual Defendants knew that the adverse facts specified herein had not been disclosed to, and/or were being concealed from, the public, and that the positive representations that were being made were then materially false and/or misleading.

18. CrowdStrike and the Individual Defendants are collectively referred to herein as "Defendants."

19. CrowdStrike is liable for the acts of the Individual Defendants, and its employees under the doctrine of *respondeat superior* and common law principles of agency as all the wrongful acts complained of herein were carried out within the scope of their employment with authorization.

20. The scienter of the Individual Defendants, and other employees and agents of the Company are similarly imputed to CrowdStrike under *respondeat superior* and agency principles.

V. COMPANY BACKGROUND

21. Founded in 2011, CrowdStrike is incorporated in Delaware and headquartered in Austin, Texas. CrowdStrike is a global cybersecurity company that provides software that helps prevent data breaches. CrowdStrike's customers are major corporations across several industries including airlines, banks, hospitals, and telecommunications providers as well as government entities.

22. CrowdStrike's main product is the Falcon software platform, which purportedly uses artificial intelligence and machine learning technologies to detect, prevent, and respond to security breach threats. CrowdStrike claims that the key to the Company's technological and business advantages is that Falcon can keep pace with cybersecurity threats through rapid innovation. CrowdStrike claims this platform constantly gathers data and analyzes cybersecurity events to "create actionable data, identify shifts in adversary tactics, and automatically prevent threats in real-time across our customer base." CrowdStrike further claims its platform is "continuously improv[ing]," to "keep customers ahead of changing adversary tactics."

23. The Falcon software is embedded in the computers of CrowdStrike's customers and requires constant updates. CrowdStrike updates its Falcon platform in at least two ways. First, there are "Sensor Content" updates that directly update Falcon's sensor. Second, there are "Rapid Response Content" updates that update how those sensors behave in trying to detect threats.

VI. MATERIAL MISREPRESENTATIONS AND OMISSIONS DURING THE CLASS PERIOD

24. The Class Period begins on November 29, 2023, the day after CrowdStrike announced its financial results for the third quarter of fiscal year 2024.[1] In connection with the release of these results, Defendants participated in a related earnings call with analysts and investors. On that call, Defendant Kurtz touted Falcon, claiming it "has made cybersecurity easy and effective for small businesses to the world's largest enterprises" and that the "drumbeat of innovation was loud and clear with multiple releases and announcements showcasing CrowdStrike as the XDR leader, including the Falcon platform Raptor release." Defendant Kurtz claimed that "from hygiene to patching, Falcon for IT lets customers consolidate multiple use cases and replace legacy products with our single-agent architecture," and touted the Company's "new Falcon Data Protection module that liberates customers from legacy [data loss prevention] products with modern, frictionless data security."

25. Also on November 29, 2023, the Company filed with the SEC a Form 10-Q reporting the Company's financial and operational results for the third quarter of fiscal year 2024 ended October 31, 2023 (the "Q3 2024 10-Q").

26. The Q3 2024 10-Q identified risk factors to the Company's business, including:

> ***If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.***
>
> Real or perceived defects, errors or vulnerabilities in our Falcon platform and cloud modules, the failure of our platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration of our solutions, or the failure of customers to take action on attacks identified by our platform could harm our

[1] CrowdStrike's fiscal year ends on January 31 each year.

reputation and adversely affect our business, financial position and results of operations.

. . .

We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.

Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform:

. . .

- errors, defects or performance problems in our software, including third-party software incorporated in our software;
- improper deployment or configuration of our solutions;
- the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and
- the failure of our disaster recovery and business continuity arrangements.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could

> result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.
>
> (emphasis in original).

27. Appended as an exhibit to the Q3 2024 10-Q were signed certifications pursuant to the Sarbanes-Oxley Act of 2002 ("SOX"), wherein the Individual Defendants certified that "[t]he [Q3 2024 10-Q] fully complies with the requirements of Section 13(a) or 15(d) of the [Exchange Act]" and that the "information contained in the [Q3 2024 10-Q] fairly presents, in all material respects, the financial condition and results of operations of [the Company]."

28. Then, on March 5, 2024, the Company announced its financial results for its fiscal year 2024 ended January 31, 2024. As part of these results, Defendants participated in a related earnings call the same day. On that call, Defendant Kurtz again touted Falcon, claiming it "is validated, tested and certified." Defendant Kurtz also highlighted CrowdStrike's "execution and discipline across the business."

29. Then, on March 7, 2024, the Company filed with the SEC a Form 10-K reporting the Company's financial and operational results for the fiscal year 2024 ended January 31, 2024 (the "2024 10-K").

30. The 2024 10-K stated:

> We offer our customers compelling business value that includes ease of adoption, rapid time-to-value, superior efficacy rates in detecting threats and preventing breaches, and reduced total cost of ownership by consolidating legacy, siloed, and multi-agent security products in a single solution. We also allow thinly-stretched security organizations to automate previously manual tasks, freeing them to focus on their most important objectives. With the Falcon platform, organizations can transform how they combat threats, transforming from slow, manual, and reactionary to fast, automated, and predictive, while gaining visibility across the threat lifecycle.
>
> Key benefits of our approach and the CrowdStrike Falcon platform include:
>
> . . .
>
> •High Efficacy, Low False Positives: The vast telemetry of the Security Cloud and the best practices employed in continually training our AI models results in industry-leading efficacy rates and low false positives.
>
> •Consolidation of Siloed Products: Integrating and maintaining numerous security products creates blind spots that attackers can exploit, is costly to maintain and negatively impacts user performance. Our cloud-native platform approach gives customers a unified approach to address their most critical areas of risk seamlessly. We empower customers to rapidly deploy and scale industry leading technologies across endpoint detection and response ("EDR") and Extended Detection and Response ("XDR"), Identity Threat Protection, Threat Intelligence, Exposure Management, Cloud Security, Application Security Posture Management, Next-Generation SIEM and Modern Log Management, and IT Automation from a single platform.
>
> •Reducing Agent Bloat: Our single intelligent lightweight agent enables frictionless deployment of our platform at scale, enabling customers to rapidly adopt our technology across any type of workload running on a variety of endpoints. The agent is non-intrusive to the end user, requires no reboots and continues to protect the endpoint and track activity even when offline. Through our single lightweight agent approach, customers can adopt multiple platform modules to address their critical areas of risk without burdening the endpoint with multiple agents. Legacy approaches often require multiple agents as they layer on new capabilities. This can severely impact user performance and create barriers to security.

•Rapid Time to Value: Our cloud-native platform was built to rapidly scale industry leading protection across the entire enterprise, eliminating lengthy implementation periods and professional services engagements that next-gen and legacy competitors may require. Our single agent, collect once and re-use many times approach enables us to activate new modules in real time.

•Elite Security Teams as a Force Multiplier: As adversaries continue to employ sophisticated malwareless attacks that exploit user credentials and identities, automation and autonomous security are no longer sufficient on their own. Stopping today's sophisticated attacks requires a combination of powerful automation and elite threat hunting. Falcon Complete provides a comprehensive monitoring, management, response, and remediation solution to our customers and is designed to bring enterprise level security to companies that may lack enterprise level resources.

CrowdStrike Falcon OverWatch, part of CrowdStrike Counter Adversary Operations, combines world-class human intelligence from our elite security experts with the power of the Falcon platform. OverWatch is a force multiplier that extends the capabilities and improves the productivity of our customers' security teams. Because our world-class team can see attacks across our entire customer base, their expertise is enhanced by their constant visibility into the threat landscape. Additionally, the insights of our OverWatch team can then be leveraged by the Falcon platform to further enhance its autonomous capabilities, creating a positive feedback loop for our customers.

•Alleviating the Skills Shortage through Automation: CrowdStrike automates manual tasks to free security teams to focus on their most important job – stopping the breach. Our Falcon Fusion capability automates workflows to reduce the need to switch between different security tools and tasks, while our Falcon Insight XDR module provides a unified solution that enables security teams to rapidly and efficiently identify, hunt, and eliminate threats across multiple security domains using first and third party datasets.

•Lower Total Cost of Ownership: Our cloud-native platform eliminates our customers' need for initial or ongoing purchases of hardware and does not require their personnel to configure, implement or integrate disparate point products. Additionally, our comprehensive platform reduces overall personnel costs associated with ongoing maintenance, as well as the need for software patches and upgrades for separate products.

. . .

Our research and development organizations are responsible for the design, architecture, operation and quality of our cloud native Falcon platform. In addition, the research and development organizations work closely with our customer success teams to promote customer satisfaction.

Our success is a result of our continuous drive for innovation. Our internal team of security experts, researchers, intelligence analysts, and threat hunters continuously analyzes the evolving global threat landscape to develop products that defend against today's most sophisticated and stealthy attacks and report on emerging security issues. We invest substantial resources in research and development to enhance our Falcon platform, and develop new cloud modules, features and functionality. We believe timely development of new, and enhancement of our existing products, services, and features is essential to maintaining our competitive position. We work closely with our customers and channel partners to gain valuable insight into their security management practices to assist us in designing new cloud modules and features that extend the capability of our platform. Our technical staff monitors and tests our software on a regular basis, and we also make our Falcon platform available for third-party validation. We also maintain a regular release process to update and enhance our existing solutions. In addition, we engage security consulting firms to perform periodic vulnerability analysis of our solutions.

. . .

Our cybersecurity risk management program, which includes data privacy, product security, and information security, is designed to align with our industry's best practices.

(emphasis in original).

31. The 2024 10-K also identified risk factors to the Company's business, including:

If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.

Real or perceived defects, errors or vulnerabilities in our Falcon platform and cloud modules, the failure of our platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration of our solutions, or the failure of customers to take action on attacks identified by our platform could harm our

reputation and adversely affect our business, financial position and results of operations.

. . .

We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.

Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform:

. . .

- errors, defects or performance problems in our software, including third-party software incorporated in our software;
- improper deployment or configuration of our solutions;
- the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and
- the failure of our disaster recovery and business continuity arrangements.

The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could

> result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.
>
> (emphasis in original).

32. Appended as an exhibit to the 2024 10-K were signed certifications pursuant to SOX, wherein the Individual Defendants certified that "[t]he [2024 10-K] fully complies with the requirements of Section 13(a) or 15(d) of the [Exchange Act]" and that the"information contained in the [2024 10-K] fairly presents, in all material respects, the financial condition and results of operations of [the Company]."

33. Also on March 7, 2024, Defendant Kurtz spoke at the Morgan Stanley Technology, Media & Telecom Conference. During that conference, he claimed it was "friction-free to deploy [CrowdStrike's product]."

34. Then, on June 5, 2024, the Company filed with the SEC a Form 10-Q reporting the Company's financial and operational results for the first quarter of fiscal year 2025 ended April 30, 2024 (the "Q1 2025 10-Q").

35. The Q1 2025 10-Q identified risk factors to the Company's business, including:

> ***If our solutions fail or are perceived to fail to detect or prevent incidents or have or are perceived to have defects, errors, or vulnerabilities, our brand and reputation would be harmed, which would adversely affect our business and results of operations.***

Real or perceived defects, errors or vulnerabilities in our Falcon platform and cloud modules, the failure of our platform to detect or prevent incidents, including advanced and newly developed attacks, misconfiguration of our solutions, or the failure of customers to take action on attacks identified by our platform could harm our reputation and adversely affect our business, financial position and results of operations.

. . .

We rely on third-party data centers, such as Amazon Web Services, and our own colocation data centers to host and operate our Falcon platform, and any disruption of or interference with our use of these facilities may negatively affect our ability to maintain the performance and reliability of our Falcon platform which could cause our business to suffer.

Our customers depend on the continuous availability of our Falcon platform. We currently host our Falcon platform and serve our customers using a mix of third-party data centers, primarily Amazon Web Services, Inc., or AWS, and our data centers, hosted in colocation facilities. Consequently, we may be subject to service disruptions as well as failures to provide adequate support for reasons that are outside of our direct control. We have experienced, and expect that in the future we may experience interruptions, delays and outages in service and availability from time to time due to a variety of factors, including infrastructure changes, human or software errors, website hosting disruptions and capacity constraints.

The following factors, many of which are beyond our control, can affect the delivery, availability, and the performance of our Falcon platform:

. . .

- errors, defects or performance problems in our software, including third-party software incorporated in our software;
- improper deployment or configuration of our solutions;
- the failure of our redundancy systems, in the event of a service disruption at one of our data centers, to provide failover to other data centers in our data center network; and
- the failure of our disaster recovery and business continuity arrangements.

> The adverse effects of any service interruptions on our reputation, results of operations, and financial condition may be disproportionately heightened due to the nature of our business and the fact that our customers have a low tolerance for interruptions of any duration. Interruptions or failures in our service delivery could result in a cyberattack or other security threat to one of our customers during such periods of interruption or failure. Additionally, interruptions or failures in our service could cause customers to terminate their subscriptions with us, adversely affect our renewal rates, and harm our ability to attract new customers. Our business would also be harmed if our customers believe that a cloud-based SaaS-delivered endpoint security solution is unreliable. While we do not consider them to have been material, we have experienced, and may in the future experience, service interruptions and other performance problems due to a variety of factors. The occurrence of any of these factors, or if we are unable to rapidly and cost-effectively fix such errors or other problems that may be identified, could damage our reputation, negatively affect our relationship with our customers or otherwise harm our business, results of operations and financial condition.
>
> (emphasis in original).

36. Appended as an exhibit to the Q1 2025 10-Q were signed certifications pursuant to SOX, wherein the Individual Defendants certified that "[t]he [Q1 2025 10-Q] fully complies with the requirements of Section 13(a) or 15(d) of the [Exchange Act]" and that the "information contained in the [Q1 2025 10-Q] fairly presents, in all material respects, the financial condition and results of operations of the [Company]."

37. The statements in ¶¶24-36 were materially false and misleading when made because, throughout the Class Period, Defendants had failed to disclose that: (1) CrowdStrike had instituted deficient controls in its procedure for updating Falcon, and was not properly testing updates to Falcon before rolling them out to customers; (2) this inadequate software testing created a substantial risk that an update to Falcon could cause major outages for a significant number of the Company's customers; and (3) such outages could pose, and in fact ultimately created, substantial reputational harm and legal risk to CrowdStrike.

VII. THE TRUTH EMERGES

38. Investors began to learn the truth behind Defendants' misrepresentations on July 19, 2024, when news broke that a flawed Falcon content update caused major worldwide technology outages for millions of devices running Microsoft Windows (the "CrowdStrike Outage"). About 8.5 million Windows devices were affected by this outage. Victims of the CrowdStrike Outage included both large corporations and government entities. Among several other consequences of the CrowdStrike Outage, airlines were forced to ground countless flights and emergency 911 hotlines were inoperable. The flawed update responsible for the CrowdStrike Outage occurred in its Rapid Response Content file. CrowdStrike also informed its customers that bad actors were trying to exploit the CrowdStrike Outage to hack CrowdStrike customers. The CrowdStrike Outage subjected CrowdStrike to substantial legal liability and massive reputational damages. On this news, shares of CrowdStrike fell ***$38.09***, or ***11%***, to close at $304.96 on July 19, 2024.

39. Then, on July 22, 2024, the reputational harm and legal risk imposed on CrowdStrike by the outage was further revealed as Congress called on Defendant Kurtz to testify regarding the crisis and the Company's stock rating was downgraded by analysts such as Guggenheim and BTIG. On this news, shares of CrowdStrike fell ***$41.05***, or ***13.5%***, to close at $263.91 on July 22, 2024.

40. Investors continued to learn about the legal risk Defendants had concealed on July 29, 2024, as news outlets reported that Delta Air Lines had hired prominent attorney David Boies to seek damages from the Company following the CrowdStrike Outage. On this news, shares of CrowdStrike fell ***$25.16***, or ***10%***, to close at $233.65 on July 30, 2024.

41. Since the CrowdStrike Outage, publicly revealed evidence indicates that CrowdStrike was taking insufficient precautions regarding such updates. For instance,

CrowdStrike has promised to take remedial measures to ensure that such a crash does not happen again, including implementing a so-called canary deployment of such updates, meaning a progressive rollout that starts with a subset of users. This indicates CrowdStrike was not taking such measures prior to the CrowdStrike Outage.

42. Expert commentary since the outage has also provided evidence of CrowdStrike's poor safety procedures. For instance, *The Verge* commented that CrowdStrike appears not to do as much thorough testing on its Rapid Response Content updates as it does on other updates. An expert quoted by *The Verge* stated that "[i]f CrowdStrike had properly tested its content updates," the CrowdStrike Outage would likely not have occurred.

43. Similarly, a cybersecurity expert cited by *Forbes* criticized CrowdStrike's quality assurance procedures and stated that "there's no absolving CrowdStrike from responsibility of this incident." An expert cited by *The Washington Post* said it was "alarming" that the CrowdStrike update was not "tested and validated" before it was implemented.

VIII. CLASS ACTION ALLEGATIONS

44. Plaintiff brings this class action under Federal Rule of Civil Procedure 23 on behalf of themselves and a class of all persons and entities who purchased or otherwise acquired CrowdStrike stock during the Class Period (the "Class"). Excluded from the Class are Defendants, their agents, directors and officers of CrowdStrike, and their families and affiliates.

45. The members of the Class are so numerous that joinder of all members is impracticable. The disposition of their claims in a class action will provide substantial benefits to the parties and the Court. As of May 30, 2024, there were approximately 231 million shares of CrowdStrike Class A common stock outstanding, owned by thousands of investors. Throughout the Class Period, CrowdStrike stock was actively traded on the NASDAQ. While the exact number of Class members is unknown to Plaintiff at this time and can be ascertained only through

appropriate discovery, Plaintiff believes that there are thousands of members in the proposed Class. Record owners and other members of the Class may be identified from records maintained by CrowdStrike or its transfer agent and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions.

46. There is a well-defined community of interest in the questions of law and fact involved in this case. Questions of law and fact common to the members of the Class, which predominate over questions which may affect individual Class members, include:

(a) Whether Defendants violated the Exchange Act;

(b) Whether Defendants omitted and/or misrepresented material facts;

(c) Whether Defendants' statements omitted material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading;

(d) Whether Defendants knew or recklessly disregarded that their statements were false and misleading;

(e) Whether the price of CrowdStrike stock was artificially inflated; and

(f) The extent of damage sustained by members of the Class and the appropriate measure of damages.

47. Plaintiff's claims are typical of those of the Class because Plaintiff and the Class sustained damages from Defendants' wrongful conduct.

48. Plaintiff will adequately protect the interests of the Class and has retained counsel who are experienced in securities class actions. Plaintiff has no interests that conflict with those of the Class.

49. A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Joinder of all Class members is impracticable.

IX. ADDITIONAL SCIENTER ALLEGATIONS

50. As alleged herein, Defendants acted with scienter in that Defendants knew, or recklessly disregarded, that the documents and public statements they issued and disseminated to the investing public in the name of the Company, or in their own name, during the Class Period were materially false and misleading. Defendants knowingly and substantially participated or acquiesced in the issuance or dissemination of such statements and documents as primary violations of the federal securities laws. Defendants, by virtue of their receipt of information reflecting the true facts regarding CrowdStrike, and their control over and/or receipt and/or modification of CrowdStrike's materially false and misleading statements, were active and culpable participants in the fraudulent scheme alleged herein.

51. Defendants knew or recklessly disregarded the false and misleading nature of the information they caused to be disseminated to the investing public. The fraudulent scheme described herein could not have been perpetrated during the Class Period without the knowledge and complicity of, or at least the reckless disregard by, personnel at the highest levels of the Company, including the Individual Defendants.

52. The Individual Defendants, because of their positions with CrowdStrike, controlled the contents of CrowdStrike's public statements during the Class Period. The Individual Defendants were each provided with or had access to the information alleged herein to be false and misleading prior to or shortly after its issuance and had the ability and opportunity to prevent its issuance or cause it to be corrected. Because of their positions and access to material, non-public information, the Individual Defendants knew or recklessly disregarded that the adverse facts specified herein had not been disclosed to and were being concealed from the investing public and

that the positive representations that were being made were false and misleading. As a result, each of the Individual Defendants is responsible for the accuracy of CrowdStrike's corporate statements and is, therefore, responsible and liable for the representations contained therein.

X. LOSS CAUSATION/ECONOMIC LOSS

53. During the Class Period, as detailed herein, CrowdStrike and the Individual Defendants made false and misleading statements and omissions, and engaged in a scheme to deceive the market. These false and misleading statements and omissions artificially inflated the price of CrowdStrike stock and operated as a fraud or deceit on the Class. Later, when Defendants' prior misrepresentations and fraudulent conduct were disclosed to the market, the price of CrowdStrike stock fell significantly. As a result of their purchases of CrowdStrike stock during the Class Period, Plaintiff and the Class suffered economic loss, *i.e.*, damages, under the federal securities laws.

XI. APPLICABILITY OF PRESUMPTION OF RELIANCE: FRAUD ON THE MARKET

54. Plaintiff will rely upon the presumption of reliance established by the fraud-on-the-market doctrine in that, among other things:

(a) Defendants made public misrepresentations or failed to disclose material facts during the Class Period;

(b) the omissions and misrepresentations were material;

(c) the Company's stock traded in an efficient market;

(d) the misrepresentations alleged would tend to induce a reasonable investor to misjudge the value of the Company's stock; and

(e) Plaintiff and other members of the Class purchased CrowdStrike stock between the time Defendants misrepresented or failed to disclose material facts and the time the true facts were disclosed, without knowledge of the misrepresented or omitted facts.

55. At all relevant times, the market for CrowdStrike stock was efficient for the following reasons, among others:

(a) as a regulated issuer, CrowdStrike filed periodic public reports with the SEC;

(b) CrowdStrike regularly communicated with public investors via established market communication mechanisms, including through regular disseminations of press releases on the major newswire services and through other wide-ranging public disclosures, such as communications with the financial press, securities analysts, and other similar reporting services;

(c) CrowdStrike was followed by numerous securities analysts employed by major brokerage firms who wrote reports that were distributed to the sales force and certain customers of their respective brokerage firms and that were publicly available and entered the public marketplace; and

(d) CrowdStrike stock was actively traded in an efficient market, including its common stock that was traded on the NASDAQ, under the ticker symbol "CRWD."

56. As a result of the foregoing, the market for CrowdStrike stock promptly digested current information regarding CrowdStrike from publicly available sources and reflected such information in CrowdStrike stock prices. Under these circumstances, all purchasers of CrowdStrike stock during the Class Period suffered similar injury through their purchase of CrowdStrike stock at artificially inflated prices and the presumption of reliance applies.

57. Further, to the extent that the Defendants concealed or improperly failed to disclose material facts with regard to the Company, Plaintiff and the Class are entitled to a presumption of reliance in accordance with *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128, 153-54 (1972).

XII. NO SAFE HARBOR

58. The statutory safe harbor provided for forward-looking statements under certain circumstances does not apply to any of the allegedly false statements pleaded in this Complaint. The statements alleged to be false and misleading herein all relate to then-existing facts and conditions. In addition, to the extent certain of the statements alleged to be false may be characterized as forward-looking, they were not identified as "forward-looking statements" when made and there were no meaningful cautionary statements identifying important factors that could cause actual results to differ materially from those in the purportedly forward-looking statements. In the alternative, to the extent that the statutory safe harbor is determined to apply to any forward-looking statements pleaded herein, Defendants are liable for those false forward-looking statements because at the time each of those forward-looking statements were made, the speaker had actual knowledge that the forward-looking statement was materially false or misleading, and/or the forward-looking statement was authorized or approved by an executive officer of CrowdStrike who knew that the statement was false when made.

XIII. CLAIMS AGAINST DEFENDANTS

COUNT I

Violations of Section 10(b) of the Exchange Act and SEC Rule 10b-5 Promulgated Thereunder Against All Defendants

59. Plaintiff incorporates by reference the allegations in the preceding paragraphs.

60. This Count is asserted against Defendants and is based upon Section 10(b) of the Exchange Act, 15 U.S.C. § 78j(b), and Rule 10b-5 promulgated thereunder by the SEC.

61. During the Class Period, Defendants disseminated or approved the false statements specified above, which they knew or recklessly disregarded were misleading in that they contained misrepresentations and failed to disclose material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading.

62. Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 in that they:

(a) Employed devices, schemes, and artifices to defraud;

(b) Made untrue statements of material facts or omitted to state material facts necessary in order to make the statements made, in light of the circumstances under which they were made, not misleading; or

(c) Engaged in acts, practices, and a course of business that operated as a fraud or deceit upon Plaintiff and others similarly situated in connection with their purchases of CrowdStrike stock during the Class Period.

63. Plaintiff and the Class have suffered damages in that, in reliance on the integrity of the market, they paid artificially inflated prices for CrowdStrike stock. Plaintiff and the Class would not have purchased CrowdStrike stock at the prices they paid, or at all, if they had been aware that the market prices had been artificially and falsely inflated by Defendants' misleading statements.

64. As a direct and proximate result of these Defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their purchases of CrowdStrike stock during the Class Period.

65. By virtue of the foregoing, Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5, promulgated thereunder.

COUNT II

Violations of Section 20(a) of the Exchange Act Against the Individual Defendants

66. Plaintiff repeats and realleges the allegations contained in ¶¶ 1-58 as if fully set forth herein.

67. The Individual Defendants acted as controlling persons of CrowdStrike within the meaning of Section 20(a) of the Exchange Act. By virtue of their positions and their power to control public statements about CrowdStrike, the Individual Defendants had the power and ability to control the actions of CrowdStrike and its employees. By reason of such conduct, Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act.

XIV. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Class, respectfully prays for judgment against Defendants as follows:

A. Determining that this action is a proper class action, designating Plaintiff as Lead Plaintiff and certifying Plaintiff as a class representative under Rule 23 of the Federal Rules of Civil Procedure and Plaintiff's counsel as Lead Counsel;

B. Awarding Plaintiff and the Class compensatory damages against all Defendants, jointly and severally, for all damages sustained as a result of Defendants' wrongdoing, in an amount to be proven at trial, together with pre-judgment interest thereon;

C. Awarding Plaintiff and the Class their reasonable costs and expenses incurred in this action, including, but not limited to, attorneys' fees and costs incurred by consulting and testifying expert witnesses; and

D. Granting such other, further, and/or different relief as the Court deems just and proper.

XV. JURY DEMAND

Plaintiff demands a trial by jury.

DATED: July 30, 2024