Wilmer J. Harris, SBN 150407
wharris@sshhzlaw.com
Amanda E. Johnson, SBN 342500
ajohnson@sshhzlaw.com
SCHONBRUN SEPLOW HARRIS HOFFMAN & ZELDES LLP
715 Fremont Avenue, Suite A
South Pasadena, CA. 91030
Telephone: (626) 441-4129
Facsimile: (626) 283-5770

Attorneys for Plaintiff, Attaullah Baig

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

ATTAULLAH BAIG,

Plaintiff,

vs.

META PLATFORMS, INC., a corporation; PINAKI MUKERJI; MARK TSIMELZON; NITIN GUPTA; WILL CATHCART; MARK ZUCKERBERG; and DOES 1-10, inclusive,

Defendants.

Case No. 3:25-cv-7604

COMPLAINT FOR VIOLATIONS OF THE SARBANES-OXLEY ACT OF 2002 (18 U.S.C. § 1514A)

DEMAND FOR JURY TRIAL

Plaintiff, Attaullah Baig, alleges as follows:

JURISDICTION AND VENUE

1. This Court has jurisdiction over the subject matter of Plaintiff's claims arising under federal law pursuant to 28 U.S.C. § 1331.

2. Venue is proper in this District Court pursuant to 28 U.S.C. § 1391(b)(2) as the events giving rise to the claims asserted herein occurred in this District.

PARTIES

3. Mr. Baig was the Head of Security, WhatsApp at Defendant Meta Platforms, Inc. ("Meta"). Prior to his employment with Meta, Mr. Baig had acquired substantial expertise in cybersecurity with employment at PayPal, Capital One, Whole Foods, among others. He is a resident of the state of Texas. At all times relevant to this Complaint, Mr. Baig was a covered employee within the meaning of SOX.

4. Defendant Meta Platforms, Inc. ("Meta") is a covered employer under SOX because it is a publicly traded company with equity securities that are registered with the U.S. Securities and Exchange Commission ("SEC") under the Securities Act of 1933, as amended, (the "Securities Act)," and which are traded on the NASDAQ Stock Exchange (NASDAQ: META). Pursuant to section 15(d) the Securities Exchange Act of 1934 (the "Exchange Act"), Meta is required to file periodic quarterly (Form 10-Q) and annual (Form 10-K) reports with the SEC.

5. Defendant Pinaki Mukerji was Director of Engineering, WhatsApp at Meta and was Mr. Baig's supervisor from June 2021 through May 2024.

6. Defendant Mark Tsimelzon is the current Director of Engineering, WhatsApp at Meta and was Mr. Baig's supervisor from May 2024 through February 2025.

7. Defendant Nitin Gupta is the current Vice President, Head of Engineering, WhatsApp at Meta.

8. Defendant Will Cathcart is the current Vice President, Head of WhatsApp at Meta.

9. Defendant Mark Zuckerberg is the current Chief Executive Officer of Meta.

10. Defendants Mukerji, Tsimelzon, Gupta, Cathcart, and Zuckerberg are hereto referred to

as "Individual Defendants."

EXHAUSTION

11. Mr. Baig and Defendant Meta entered into a tolling agreement dated May 6, 2023, in order to extend the deadline to file a complaint with the Department of Labor's Occupational Safety and Health Administration ("OSHA") under SOX based on a verbal warning Mr. Baig received on November 14, 2022. This tolling agreement, originally set to expire 180 days after the May 6, 2023, effective date, has since been amended nine times to extend this and all other filing deadlines. The most recent extension of this tolling agreement expired on January 15, 2025.

12. On January 17, 2025, Mr. Baig filed a pre-termination complaint with OSHA. OSHA acknowledged the complaint and determined that the filing was timely, thus preserving all the previous claims dating back to at least November 14, 2022.

13. Mr. Baig received a notice of termination of employment due to poor performance on February 10, 2025. On April 11, 2025 Mr. Baig filed an additional SOX complaint based on his termination. The OSHA actions were consolidated by an order on May 6, 2025. This new adverse action falls within the 180-day statute of limitations for claims under SOX.

14. More than 180 days have passed since Mr. Baig filed his OSHA complaint on January 17, 2025, without a final decision.

15. On September 8, 2025, Plaintiff submitted his Notice of Intent to Remove his Sarbanes-Oxley claims to federal court. Accordingly, Plaintiff has exhausted his administrative remedies prior to bringing this action.

FACTUAL ALLEGATIONS

16. Mr. Baig observed what he reasonably believed to be several violations of the Sarbanes Oxley Act, including, without limitation, failure to disclose information security issues, potentially committing shareholder fraud, violations of SEC rules relating to internal controls, and/or failure to disclose material weaknesses in internal controls related to information security under Sections 302 and 404 of the Act.

//

A. Initial Discovery and Early Reporting (2021-2022)

17. Beginning in September 2021, shortly after joining WhatsApp as Head of Security, Mr. Baig discovered systemic cybersecurity failures that posed serious risks to user data and violated Meta's legal obligations under the 2020 Privacy Order and federal securities laws. Through a "Red Team Exercise" conducted with Meta's Central Security team, Mr. Baig discovered that approximately 1,500 WhatsApp engineers had unrestricted access to user data, including sensitive personal information covered by the FTC Privacy Order, and could move or steal such data without detection or audit trail.

18. From September 2021 through September 2022, on approximately five separate occasions, Mr. Baig raised concerns with his supervisor Suren Verma that WhatsApp lacked fundamental cybersecurity knowledge required for regulatory compliance, specifically: (a) what user data it was collecting; (b) where and how it was storing such data; and (c) who had access to it. Mr. Verma consistently ignored these concerns and directed Mr. Baig to focus on less critical application security tasks.

19. In February 2022, recognizing the urgent need for systemic data protection, Mr. Baig created a comprehensive product requirements document for the Privacy Infrastructure team to build a data classification and handling system necessary for compliance with the 2020 Privacy Order. This represented the first concrete step toward addressing WhatsApp's fundamental data governance failures. Mr. Baig understood that Meta's culture is like that of a cult where one cannot question any of the past work especially when it was approved by someone at a higher level than the individual who is raiding the concern.

B. Formal Escalation to Senior Leadership (August-October 2022)

20. On August 18, 2022, following two cybersecurity incidents affecting WhatsApp users, Mr. Baig met with Will Cathcart, Vice President, and Head of WhatsApp, along with other senior executives including Vice President of Global Communications Carl Woog, Director & Associate General Counsel Jessica Romero, and Associate General Counsel Brady Freeman. In this meeting, Mr. Baig disclosed WhatsApp's dangerous cybersecurity understaffing and systemic security failures,

specifically informing Mr. Cathcart that WhatsApp had only ten engineers working on security while comparably sized companies required approximately two hundred security professionals.

21. At Mr. Cathcart's express request, Mr. Baig prepared a comprehensive pre-read document detailing WhatsApp's cybersecurity deficiencies for a follow-up meeting. On September 8, 2022, Mr. Baig shared with the meeting attendees this document, which identified six critical cybersecurity failures that violated the 2020 Privacy Order and potentially constituted securities fraud:

a. **Failure to inventory user data:** WhatsApp lacked a comprehensive list of all user data elements collected, violating disclosure requirements under California Consumer Privacy Act (CCPA), European Union GDPR, and the 2020 Privacy Order's mandate for a comprehensive privacy program;

b. **Failure to locate data storage:** WhatsApp lacked a comprehensive inventory of systems storing user data, preventing proper protection and regulatory disclosure;

c. **Unrestricted data access:** Approximately 1,500 engineers had unfettered access to Covered Information under the 2020 Privacy Order without business justification, violating FTC requirements for access controls limited to employees with documented business need;

d. **Absence of access monitoring:** WhatsApp lacked systems to monitor user data access, preventing detection of suspicious activity and violating the 2020 Privacy Order's requirement for comprehensive privacy program protection;

e. **Inability to detect data breaches:** WhatsApp lacked 24/7 Security Operations Center capabilities standard for companies of its size and complexity, violating the 2020 Privacy Order's requirement for information security programs designed to protect Covered Information; and

f. **Massive daily account compromises:** Approximately 100,000 WhatsApp users daily suffered account takeovers with access to Covered Information, yet WhatsApp failed to implement adequate preventive measures.

22. In his pre-read document, Mr. Baig explicitly warned of legal consequences, stating: "We have a fiduciary responsibility to protect our users and their data. The penalties can be severe both

in terms of brand damage and fines," directly referencing the SEC and FTC settlements that had resulted in unprecedented penalties for similar failures.

23. On October 18, 2022, despite ongoing retaliation from his supervisors and directed by leadership at Meta, Mr. Baig presented his findings to approximately ten WhatsApp senior executives, including Mr. Cathcart, Nitin Gupta (Vice President, Head of Engineering), and other Vice Presidents. During this presentation, Mr. Baig warned that WhatsApp would face lawsuits due to data breaches if these systemic failures were not addressed. Global Public Policy Head Jonathan Lee explicitly acknowledged the gravity of the situation by asking whether WhatsApp would face the same consequences as "Mudge at Twitter," referencing the high-profile Twitter whistleblower case involving Congressional investigation and FTC enforcement action for similar cybersecurity failures.

24. Following the October 18, 2022 meeting, Mr. Baig sent all attendees a Forbes article about Twitter whistleblower Peiter Zatko, whose cybersecurity disclosures had resulted in accusations of fraud and securities violations, explicitly stating that Zatko "accused the social media company of committing fraud and numerous 'egregious' security violations" and warning of stock market implications. By sharing this article, Mr. Baig made clear that the cybersecurity failures he identified constituted potential legal violations similar to those at Twitter.

C. Continued Reporting Despite Escalating Retaliation (2023)

25. On March 15, 2023, Mr. Baig met with Meta's Central Security team and reiterated all six critical cybersecurity issues identified in his earlier reports. In a subsequent document circulated after this meeting, Mr. Baig explicitly warned that WhatsApp was "at risk of additional legal action by the FTC, SEC, IDPC, and other regulators for not meeting our legal obligations" and that the company had "not seen much or any progress on the state of security for WhatsApp."

26. Throughout 2023, despite intensifying retaliation from management and systemic abuse, Mr. Baig continued raising concerns about data exfiltration risks and compliance failures. On August 30, 2023, during a check-in meeting with senior leadership, Mr. Baig directly stated that WhatsApp's failure to develop systems to detect and respond to external attacks would violate the 2020 Privacy Order.

27. On September 11, 2023, at a model building workshop, Mr. Baig led discussions about cybersecurity gaps and compliance requirements under the FTC Privacy Order, continuing to advocate for systemic remediation of the identified failures.

28. In September 2023, Mr. Baig published an internal vision document outlining necessary steps for protecting WhatsApp user data and complying with the 2020 Privacy Order, including: (a) identifying all systems containing WhatsApp user data; (b) implementing immutable audit trails for data access; (c) reducing employee access based on documented business need; and (d) detecting anomalous data access in real time.

D. Escalation to Chief Executive Officer (2024)

29. On January 2, 2024, after systemic retaliation for his cybersecurity disclosures, Mr. Baig sent a detailed letter to Mark Zuckerberg, CEO of Meta, and Jennifer Newstead, General Counsel, documenting: (a) violations of the 2020 Privacy Order; (b) violations of SEC rules and regulations; (c) escalating retaliation against him for raising these concerns; and (d) evidence that the central security team had falsified security reports to cover up decisions not to remediate data exfiltration risks. Mr. Baig warned that such falsifications could lead to criminal penalties and provided extensive documentation of cybersecurity gaps and failed remediation efforts.

30. On January 30, 2024, Mr. Baig provided upward feedback to Nitin Gupta documenting Meta's "false commitment" to the Irish Data Privacy Commissioner regarding technical controls preventing WhatsApp user data access by Meta employees. Mr. Baig cited specific examples of data warehouse tables accessible to 20,000-65,000 employees, directly violating both the "Uber Commitment" and Section VII of the 2020 Privacy Order. It was later discovered that some data warehouse tables could be accessed by even a higher number of employees (i.e.: 100,000).

31. Throughout 2024, Mr. Baig continued documenting and reporting specific compliance failures, including: (a) profile scraping affecting over 400 million users daily without proper regulatory notification; (b) cybersecurity risks from new features that would exacerbate account takeover problems e.g.: WhatsApp Contacts; (c) under-reporting of security incidents to regulators as required by GDPR and the 2020 Privacy Order; and (d) systemic manipulation of user harm metrics to game the

performance management system and avoid addressing cybersecurity vulnerabilities.

32. In 2024, Mr. Baig and his team built several security features to reduce user harm, but Meta blocked the launch of these features:

a. Upon receiving numerous complaints from users who were being hacked and locked out of their accounts, Mr. Baig and his team built:

i. Post Compromise Account Recovery (PCR): A feature that would allow a hacked user to recover their account from their existing device.

ii. Account Defense 2.0: A feature that would require login approval from a user's existing device.

b. Upon receiving numerous reports about widespread impersonation scams on WhatsApp, Mr. Baig and his team built a feature to prevent profile photos from being scraped.

c. Mr. Baig and his team also built a feature to prevent users from being incorrectly banned and reported to National Center for Missing and Exploited Children (NCMEC). An attacker could exploit a vulnerability in WhatsApp to falsely accuse a good user of sending them child porn.

d. Mr. Baig and his team learnt that journalists and at-risk population were being attacked by nation-state actors. They built two product security features to mitigate this risk:

i. Covert Messaging: A feature that would introduce an artificial random delay in message notifications to prevent timing attacks from inferring "who is messaging who" on WhatsApp.

ii. Advance Secure Mode: A feature that would limit attackers from sending malware to the targeted user's device.

E. External Regulatory Filings (2024-2025)

33. On November 27, 2024, after exhausting internal remedies and facing continued retaliation, Mr. Baig filed a Form TCR with the Securities and Exchange Commission documenting Meta's cybersecurity deficiencies and failure to inform investors about material cybersecurity risks. Mr. Baig reported that Meta had failed to track and manage user data collection, identify data storage

locations, and address systemic scraping and account takeover issues known to senior leadership.

34. On December 4, 2024, Mr. Baig sent a second letter to Mr. Zuckerberg documenting continued cybersecurity problems and escalating retaliation, informing the CEO that he had filed the SEC complaint and requesting immediate action to address both the underlying compliance failures and the unlawful retaliation. Mr. Baig also urged Mr. Zuckerberg to put the interests of Meta user's first as opposed to treating them as numbers on some dashboard, "I think there is something important missing from "Meta, Metamates, Me" and in my opinion that is what makes or breaks our company".

35. On January 17, 2025, Mr. Baig filed a complaint with the Occupational Safety and Health Administration under Section 806 of the Sarbanes-Oxley Act, documenting the systemic retaliation he had suffered for reporting cybersecurity failures and regulatory violations, and informed Meta of this filing.

36. On February 4, 2025, Mr. Baig told the internal investigator that Meta is treating his retaliation complaints as routine isolated sexual harassment claim "This is not a sexual harassment. This is about the company".

37. Throughout this period, Mr. Baig's disclosures consistently focused on conduct he reasonably believed constituted: (a) violations of SEC rules and regulations regarding internal controls and material cybersecurity risks; (b) securities fraud through misrepresentations about WhatsApp's security capabilities in public filings and statements; (c) violations of the 2020 Privacy Order constituting potential shareholder fraud; and (d) wire fraud through systemic failures to protect user data as represented to regulators and the public.

38. Each of Mr. Baig's disclosures was made in good faith based on his reasonable belief, supported by his extensive cybersecurity expertise and documented evidence, that Meta and WhatsApp were violating federal securities laws, SEC regulations, and court-ordered compliance requirements in ways that posed material risks to shareholders and constituted fraud against investors who relied on the company's representations about its cybersecurity capabilities and regulatory compliance.

//

//

F. Chronology of Retaliatory Conduct

1. Initial Retaliation Following First Cybersecurity Disclosures (September-November 2022)

39. Immediately after Mr. Baig's September 26, 2022 cybersecurity disclosure to management, Defendants began a systemic campaign of retaliation designed to punish him for his protected activity and deter future reporting. On September 26, 2022, the same day Suren Verma reviewed Mr. Baig's pre-read document detailing systemic cybersecurity failures, Mr. Verma contacted Mr. Baig via video call and made explicit retaliatory threats, stating the document was "the worst doc I have seen in my life" and warning that Nitin Gupta "would fire him for writing a document like this." Mr. Verma further threatened to withdraw support for Mr. Baig's compensation package and discretionary equity, asking rhetorically whether Mr. Baig was "going to tell Will [Cathcart] that the whole system is broken."

40. Within three days of his cybersecurity disclosure, on September 29, 2022, Mr. Baig experienced his first adverse employment action when Pinaki Mukerji, his direct supervisor, provided negative performance feedback for the first time since Mr. Baig's employment began, falsely claiming that Mr. Baig was "not performing well" and that "the quality of his written work product was insufficient." This feedback directly contradicted over a year of consistently positive performance evaluations, including Mr. Mukerji's previous praise for Mr. Baig's "[e]xtreme focus and clarity on project scope, timeline etc." in June 2022, just three months earlier.

41. Simultaneously with this negative feedback, and without Mr. Baig's knowledge, Mr. Mukerji changed Mr. Baig's performance rating to "Needs Support" for the October 2022 performance review cycle, marking the first time Mr. Baig had received anything other than positive performance designations during his tenure at Meta.

42. Beginning immediately after September 26, 2022, Mr. Mukerji initiated an intensive micromanagement campaign specifically designed to create pretextual performance issues. Whereas Mr. Mukerji had previously rarely reviewed Mr. Baig's work product and generally maintained minimal involvement in his day-to-day activities, Mr. Mukerji suddenly began: (a) demanding to

review nearly all of Mr. Baig's work product; (b) scheduling two to three additional meetings per week for the sole purpose of critiquing Mr. Baig's work; (c) actively soliciting negative feedback about Mr. Baig from his peers; and (d) creating artificial work assignments designed to manufacture opportunities for criticism.

43. On October 6, 2022, Mr. Mukerji sent Mr. Baig a harsh written message stating "I am questioning your judgment call," representing a dramatic departure from their previously collegial professional relationship. That same day, for the first time since joining Meta, Mr. Verma told Mr. Baig that he was "not meeting expectations" and required additional support, using Meta's terminology of "Needs Support" to formally document supposed performance deficiencies.

44. On October 17, 2022, during a thirty-minute performance review meeting, Mr. Mukerji repeatedly told Mr. Baig that he was in "Needs Support" territory and issued an ultimatum that Mr. Baig must secure positive feedback from the Integrity and Data Science teams by year-end or face negative impact on his annual performance rating. When Mr. Baig requested specific guidance on how to meet these requirements, both Mr. Mukerji and Mr. Verma provided only vague, non-actionable criticism focused on alleged collaboration failures.

45. The retaliation escalated to formal disciplinary action on November 14, 2022, when Mr. Mukerji and Mr. Verma presented Mr. Baig with a verbal warning alleging violations of Meta's Respectful Communication Policy. The supervisors claimed Mr. Baig had engaged in "unprofessional and disrespectful" interactions with other teams, citing "several instances where word choice, tone or volume of voice, and dismissive and/or belittling behavior has occurred." Significantly, when Mr. Baig requested specific examples of this alleged misconduct, his supervisors refused to provide details, claiming "everything is confidential" and instructing him "not to try to find out any more detail."

46. The verbal warning included specific criticism of routine cybersecurity practices, including reprimanding Mr. Baig for asking the payments team "Do you understand the risks here?" during a standard cybersecurity risk assessment—a question that represents normal professional practice in cybersecurity evaluations. The warning concluded with a threat that "any further conduct along these lines could result in further discipline," creating a documented basis for future adverse

action.

47. Meta's Employee Relations Business Partner Mona Sawani subsequently acknowledged to Mr. Baig that the verbal warning suffered from two significant procedural defects: (a) the feedback was "generic and not actionable," which she had communicated to Mr. Mukerji and Mr. Verma before they issued the warning; and (b) the timing of the underlying complaint was suspicious, as the alleged misconduct had purportedly begun in July 2022 but was not reported until October 2022, immediately following Mr. Baig's cybersecurity disclosures.

2. Performance Review Retaliation and Financial Punishment (2023)

48. Despite promises from his supervisors in early 2023 that his performance was "perfect except for the collaboration issue" and that he would receive a "Greatly Exceeds Expectations" or "Redefines Expectations" rating, Mr. Baig's February 24, 2023 annual performance review represented clear retaliation for his protected activity. Mr. Baig received a "Consistently Meets Expectations" rating, a significant downgrade from his previous "Exceeds Expectations" rating, despite having received over forty pages of peer feedback that was overwhelmingly positive.

49. Mr. Mukerji cherry-picked isolated negative comments from the extensive positive feedback and added an "Areas of Improvement" section to Mr. Baig's review—a discretionary addition that Mr. Baig had never received in previous performance evaluations. The performance review explicitly referenced the October 2022 complaint as the basis for the lowered rating, demonstrating direct causal connection between Mr. Baig's protected cybersecurity disclosures and the adverse employment action.

50. On March 3, 2023, Mr. Verma explicitly acknowledged the retaliatory nature of the performance review during a meeting with Mr. Baig, stating that Mr. Baig "likely would have received a 'Greatly Exceeds Expectations' rating had there not been any collaboration issues" and that "a number of Mr. Baig's superior peers were supportive of a higher rating and higher compensation." Mr. Verma also revealed that management had "contemplated terminating" Mr. Baig in November 2022 instead of issuing the verbal warning and warned that Mr. Baig "would be terminated if there were another incident."

51. The retaliatory performance review resulted in substantial financial harm to Mr. Baig, including: (a) denial of an earned promotion that would have increased his base salary by approximately $40,000-$45,000 annually; (b) loss of higher bonus payments tied to performance ratings; (c) denial of formulaic equity grants tied to performance level; and (d) loss of discretionary equity grants worth approximately $600,000, which Mr. Mukerji and Mr. Gupta denied despite acknowledging in the performance review that Mr. Baig had "solved problems that many people thought could not be solved" and made significant organizational contributions.

52. Throughout late February and early March 2023, Mr. Mukerji continued the retaliatory micromanagement by creating artificial work assignments, including directing Mr. Baig to recreate a document that had already been widely reviewed and then making approximately fifty comments on the resulting one-page document. Mr. Mukerji used these manufactured assignments to claim he was "coaching" Mr. Baig to develop communication skills, further documenting pretextual performance issues.

3. Escalating Retaliation and Silencing Attempts (2023-2024)

53. After Mr. Baig's March 15, 2023 meeting with Meta's Central Security team, where he again raised compliance concerns, Mr. Verma intensified efforts to silence his reporting. On March 24, 2023, during an angry confrontation, Mr. Verma explicitly directed Mr. Baig not to state in writing that WhatsApp was non-compliant with the FTC Privacy Order, claiming that Mr. Baig was "not a lawyer" and should not make such determinations. Mr. Verma expressed specific concern that if there were a lawsuit, Mr. Baig's written statements about non-compliance could become discoverable, demonstrating awareness that the cybersecurity failures constituted legal violations.

54. On April 14, 2023, Mr. Mukerji issued a direct prohibition against discussing regulatory compliance, stating: "I don't want you to talk about FTC [Privacy Order] unless it is with [WhatsApp attorney] Yannick [Carapito]. I am serious." This directive represented a clear attempt to prevent Mr. Baig from continuing his protected disclosure activity by limiting his ability to raise legal compliance concerns with appropriate personnel.

55. Throughout 2023, as Mr. Baig continued advocating for cybersecurity remediation,

Defendants expanded the retaliation to include systemic exclusion from decision-making processes. Colleagues began refusing to allow Mr. Baig to edit pre-read documents for critical security meetings, forbidding him from adding comments to meetings with senior leadership, and actively excluding his input from discussions that directly related to his cybersecurity responsibilities.

56. On July 18, 2023, Gregory Heimbuecher, a member of Meta's central security team, personally attacked Mr. Baig during a meeting, warning him: "Don't be the guy that people hate to work with" and claiming that Mr. Baig's comments about cybersecurity deficiencies made the central security team look like "idiots." This hostile response to Mr. Baig's continued advocacy for cybersecurity improvements represented part of the broader retaliatory campaign.

57. In October 2023, following Mr. Baig's continued efforts to secure internal audits of cybersecurity deficiencies, Alan Thomas, Employee Relations Business Partner, informed Mr. Baig that he had received anonymous negative feedback about his work. The feedback, which Mr. Baig reasonably suspected came from Mr. Heimbuecher based on their previous interactions, alleged that Mr. Baig questioned colleagues' competence and made unreasonable demands—allegations that directly contradicted the positive feedback Mr. Baig had received from the same individuals just months earlier.

58. On December 15, 2023, the retaliation reached new levels when multiple members of Meta's central security team, including Steve Clarke and Chad Greene, approached Mr. Mukerji to provide coordinated negative feedback about Mr. Baig. This feedback session occurred immediately after Mr. Baig raised concerns about large-scale data exfiltration risks in a Q4 2023 Quarterly Security Review, demonstrating the direct connection between his protected activity and the adverse response from management and colleagues.

4. Management Change as Retaliation Vehicle (2024)

59. In May 2024, Defendants orchestrated a management change designed to facilitate and obscure continued retaliation against Mr. Baig. Despite Mr. Mukerji's extended family leave, Meta assigned Mr. Baig to report to Mark Tsimelzon, a London-based director who had previously blocked multiple projects led by Mr. Baig and had demonstrated hostility to Mr. Baig's cybersecurity initiatives.

This reporting arrangement was highly unusual, as it required cross-timezone management and gave Mr. Tsimelzon eleven direct reports compared to the typical three direct reports for other Engineering Directors.

60. On May 29, 2024, less than one month after assuming supervisory responsibility, Mr. Tsimelzon sent Mr. Baig a letter accusing him of "serious collaboration issues" and stating that he was "not meeting expectations of his role." The letter provided no specific examples of problematic behavior, projects, or individuals, rendering the feedback non-actionable and demonstrating its pretextual nature.

61. Throughout summer 2024, Mr. Tsimelzon continued the pattern of retaliation by: (a) prohibiting Mr. Baig from discussing legal requirements related to the 2020 Privacy Order; (b) soliciting negative feedback from colleagues who had previously provided positive evaluations of Mr. Baig's work; (c) suddenly reducing the scope of Mr. Baig's responsibilities to exclude critical cybersecurity functions; and (d) blocking Mr. Baig's team from implementing successful security solutions.

62. On August 8, 2024, Mr. Tsimelzon issued Mr. Baig his first "Below Expectations" performance rating in a mid-year review that explicitly relied on Mr. Mukerji's previous retaliatory feedback from December 2023. Despite acknowledging Mr. Baig's successful implementation of new security measures, the review focused entirely on alleged "collaboration" issues based on complaints from the same individuals who had obstructed Mr. Baig's cybersecurity remediation efforts.

5. Project Sabotage and Solution Destruction (2024)

63. Throughout 2024, Defendants engaged in systemic sabotage of Mr. Baig's successful cybersecurity initiatives, demonstrating that the retaliation was designed not only to punish him personally but to prevent implementation of the security improvements he advocated. In September 2024, when Mr. Baig's team published findings that WhatsApp was leaking over 400 million user profile photos daily to scrapers, leadership refused to act on the findings, blocked progress on remediation, and refused to provide necessary staffing to address the security gap.

64. In October 2024, Mark Hatton, a Software Engineering Manager in Mr. Tzimelzon's

team, explicitly pressured one of Mr. Baig's team members to revise a cybersecurity risk assessment to minimize stated risks from a new login feature that allowed WhatsApp users to link their account with Facebook or Instagram accounts. When the team member resisted this pressure, Mr. Hatton created a group chat with Mr. Tsimelzon to accuse Mr. Baig of collaboration issues and territorial overreach for attempting to ensure accurate risk assessment.

65. The most egregious example of retaliatory project sabotage occurred in December 2024, when Mr. Tsimelzon ordered the rollback of Mr. Baig's Post Compromise Account Recovery (PCR) solution, which had successfully launched to 5% of WhatsApp users and was recovering approximately 25,000 compromised accounts daily extrapolating this meant that about 500,000 WhatsApp users were being hacked and locked out of their accounts daily. On December 19, 2024, Mr. Tsimelzon colluded with Dick Brouwer, an Engineering Director responsible for WhatsApp user growth to create artificial collaboration issues, handed the successful project to Mark Hatton's team, and ordered the solution to be discontinued, explicitly choosing retaliation over user safety.

66. When Mr. Baig's team member reached out directly to Will Cathcart in January 2025 requesting prioritization of user safety over internal politics and asking for help to restore the PCR solution, Mr. Cathcart refused to act despite multiple messages, demonstrating that the retaliation had approval from the highest levels of WhatsApp leadership.

6. Professional Sabotage and Career Destruction (2024-2025)

67. In late 2024, Defendants expanded their retaliation to target Mr. Baig's professional development and intellectual property contributions. For the first time in his career at Meta, two of Mr. Baig's patent proposals (for Post Compromise Recovery and Covert Messaging) were denied, representing a clear departure from his previous track record of successful patent applications.

68. During the 2024 year-end performance calibrations, Defendants demonstrated systemic bias by: (a) denying a well-deserved promotion to one of Mr. Baig's team members, downgrading his rating from "Greatly Exceeds" to "Exceeds" in apparent retaliation; (b) excluding Mr. Baig's team from budget allocations for 250 additional engineers that Mr. Gupta received for initiatives; and (c) allowing false performance metrics from other teams (including a fabricated claim of $1.5 billion in SMS cost

savings) while blocking recognition for Mr. Baig's team's actual security achievements.

69. Throughout late 2024 and early 2025, Mr. Tsimelzon continued censoring Mr. Baig's cybersecurity reporting, including ordering the immediate deletion of a November 2024 report that documented the ineffectiveness of existing anti-scraping measures. Mr. Tsimelzon explicitly stated that the report needed to be deleted because it would make his team "look bad to leadership," demonstrating that the suppression of Mr. Baig's work was designed to hide cybersecurity failures from senior management.

7. Termination as Ultimate Retaliation (February 2025)

70. On February 10, 2025, Defendants culminated their retaliation campaign by informing Mr. Baig that his employment would be terminated for "poor performance" as part of Meta's performance-based layoffs. This termination occurred less than two months after Mr. Baig informed Mark Zuckerberg that he had filed a Form TCR with the SEC and less than one month after he informed Meta that he had filed a SOX retaliation complaint with OSHA.

71. The termination decision required Defendants to "go to extreme lengths to justify" the performance-based termination, according to internal sources, demonstrating the pretextual nature of the stated reasons. This termination occurred despite: (a) strong positive feedback from Mr. Baig's team acknowledging the "significant adversity and retaliation" they had faced throughout 2024; (b) successful implementation of critical security measures including the PCR solution that was recovering hundreds of thousands of compromised accounts daily; and (c) continued advocacy for cybersecurity improvements that had resulted in meaningful policy changes, including updates to Meta's Annual Required Training incorporating Mr. Baig's recommendations.

72. The timing and circumstances of Mr. Baig's termination establish clear causal connection to his protected activity, occurring in close temporal proximity to his external regulatory filings and representing the culmination of over two years of systemic retaliation for his cybersecurity disclosures and advocacy for compliance with federal law and regulatory orders.

73. Throughout the entire retaliation campaign, from September 2022 through February 2025, Defendants' adverse actions consistently followed Mr. Baig's protected disclosures about

cybersecurity failures and regulatory violations, demonstrating that his whistleblowing activity was a contributing factor in each adverse employment action. The escalating pattern of retaliation, combined with explicit threats and acknowledgments from supervisors, establishes that Defendants' conduct was designed to punish Mr. Baig for his protected activity and deter continued reporting of cybersecurity and compliance failures.

FIRST CAUSE OF ACTION

RETALIATION IN VIOLATION OF 18 U.S.C. § 1514A

74. Plaintiff restates and incorporates all paragraphs as though fully set forth herein.

75. At all relevant times, DEFENDANTS issued and maintained a class of publicly traded securities registered pursuant to Section 12(b) of the Securities Exchange Act of 1934, which were traded on the New York Stock Exchange.

76. Plaintiff engaged in activity protected under 15 U.S.C. § 1514A when he, inter alia:

a. Reported what he reasonably believed to be violations of SEC rules and regulations, that had occurred, were ongoing, or were about to occur;

b. Reported what he reasonably believed to be Defendants' unlawful failure to disclose information security issues, potentially constituting shareholder fraud;

c. Reported what he reasonably believed to be violations of SEC rules relating to internal controls;

d. Reported what he reasonably believed to be Defendants' failure to disclose material weaknesses in internal controls related to information security under Sections 302 and 404 of SOX;

e. The Individual Defendants, and their respective Board of Directors, CEOs, Presidents, CFOs, and other officers and managing agents knew, should have known, or suspected that Plaintiff engaged in such protected activity.

77. Plaintiff suffered an adverse action when he was terminated.

78. Plaintiff's protected activity was a contributing factor—and indeed the reason for—his termination.

79. As a proximate result of the Defendants' actions against Plaintiff, as alleged above, Plaintiff has been harmed in that he has suffered the loss of wages, benefits, and additional amounts of money he would have received if he had not been subjected to said treatment. Plaintiff has also been harmed in that he has suffered humiliation, mental anguish, reputational damages, and emotional and physical distress. As a result of such conduct, Plaintiff has suffered damages in an amount according to proof.

80. Plaintiff also seeks litigation costs, expert witness fees, and reasonable attorney fees pursuant to 18 U.S.C. § 1514A(3)(2).

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court:

A. Enter judgment in favor of Plaintiff and against Defendants;

B. Award all relief necessary to make Plaintiff whole, including: (1) reinstatement with the same seniority status that Plaintiff would have had but for the discrimination; (2) back pay with interest; and (3) compensation for any special damages sustained as a result of the discrimination, including litigation costs, expert witness fees, and reasonable attorney fees;

C. Award compensatory damages for emotional distress, mental anguish, and other consequential damages;

D. Award prejudgment and post-judgment interest; and

E. Grant such other relief as the Court deems just and proper.

DATED: September 8, 2025

SCHONBRUN SEPLOW HARRIS HOFFMAN & ZELDES LLP

/s/Wilmer J. Harris

By: _____

Wilmer J. Harris

Amanda E. Johnson

Attorneys for Plaintiff, Attaullah Baig

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on all claims.

DATED: September 8, 2025

SCHONBRUN SEPLOW HARRIS HOFFMAN & ZELDES LLP

/s/Wilmer J. Harris

By: _____

Wilmer J. Harris

Amanda E. Johnson

Attorneys for Plaintiff, Attaullah Baig