WhatsApp Security Chief Says Up To 500,000 Accounts Compromised Daily Before Meta Retaliated And Fired Him

Attaullah Baig was hired to protect WhatsApp users on the Meta platform. Instead, he says that he discovered a system so broken that up to 500,000 accounts were being hijacked every day. He also says that it went beyond just that, and that 1,500 engineers could access anyone's personal data without leaving a trace on their systems.

He has now filed a legal complaint against Meta after he says that he was fired for exposing those vulnerabilities to the management team.

His federal lawsuit details how the company allegedly chose user growth over safety and retaliated against him for 3 years when he was trying to do the right thing.

The Red Team Discovery About Account Access

In September 2021, Baig conducted a standard security exercise with Meta's central team. The results were very bad. He found that almost 1,500 engineers with production access could steal user data including contact lists, profile photos and location information without detection.

"Any one of these roughly 1,500 engineers could find and identify an elected official's geographic location while messaging through their IP address and see the contact number of who they were messaging," Baig stated in his complaint.

He immediately reported the risk to his manager.

Account Takeover Was Horrible At Meta

When Baig began to dig further he found even more issues at Meta.

His team's data showed approximately 100,000 WhatsApp accounts were being taken over daily in 2022, a figure that grew to an estimated 500,000 by late 2024.

Despite building a solution called Post Compromise Account Recovery that could restore 25,000 hijacked accounts daily when launched to just 5% of users,

management ordered it rolled back. "If the security team fixes this, then what will we do?" Mark Hatton, a software engineering manager, reportedly told Baig when rejecting preventive security measures.

Meta Retaliated Against Him – The Worst Document I Have Seen In My Life

Baig said after he reported the risk to management they began to retaliate against him.

Within three days of his September 2022 cybersecurity report, his supervisor gave him negative performance feedback for the first time, claiming his work was "not performing well."

His manager also gave him a bad review, calling his security assessment "the worst doc I have seen in my life" and warned that the Vice President would “fire him” for writing it.

By November, he received a formal warning for allegedly unprofessional behavior, though managers refused to provide specific examples.

His Salary Was Impacted

Baig also claimed that his annual compensation took a major hit. Despite being told he would receive top ratings, his 2023 performance review was downgraded, costing him an estimated $1 million in bonuses and equity grants.

His supervisors acknowledged he had "solved problems that many people thought could not be solved" but still denied him a $600,000 discretionary equity grant. A promised promotion worth $40,000 to $45,000 in additional salary also vanished.

WhatsApp Was Scraped Badly By External Parties

In September 2024, Baig's team published findings showing WhatsApp was leaking over 400 million user profile photos daily to scrapers. According to him, leadership at Meta refused to act or provide staffing to address the gap.

When Baig tried to report this he said he was blocked internally from fully reporting it.

Gaming the System

Throughout his investigation at Meta, Baig discovered teams were manipulating user harm metrics to improve their performance ratings. One team falsely claimed saving $1.5 billion in SMS costs when the actual annual spend was only around far less.

"This company doesn't do anything for security unless forced by the FTC," Nilesh Agrawal, a senior WhatsApp engineer, told Baig in June 2024.

Another engineer, Parth Shah, admitted he couldn't work on security solutions because "this company runs on PSC," referring to Meta's performance review system.

He Was Terminated After Filing Whistleblower Complaint

After exhausting everything he could, Baig filed a whistleblower complaint with the SEC in November 2024. He wrote directly to Mark Zuckerberg twice, warning about violations of the 2020 FTC Privacy Order that had already cost Meta $5 billion.

On February 10, 2025, less than a month after filing his complaint with the Occupational Safety and Health Administration, Baig received notice of termination for "poor performance." Internal sources told him Meta had to "go to extreme lenghts to justify" the firing.

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

EXHIBIT A

UNITED STATES DEPARTMENT OF LABOR
OCCUPATIONAL SAFETY AND HEALTH ADMINISTRATION

Attaullah Baig	)
Complainant,	)
v.	)
Meta Platforms, Inc., Pinaki Mukerji, Mark Tsimelzon, Nitin Gupta, Will Cathcart, Chris Cox and Mark Zuckerberg	)
Respondents	)

COMPLAINT

1. Complainant Attaullah Baig brings this action against Respondents Meta Platforms, Inc. ("Meta" or "the Company"), Pinaki Mukerji, Mark Tsimelzon, Nitin Gupta, Will Cathcart, Chris Cox, and Mark Zuckerberg for unlawful retaliation in violation of the whistleblower protection provision of the Sarbanes-Oxley Act, 18 U.S.C. § 1514A ("SOX").

Parties

2. Mr. Baig is the Head of Security, WhatsApp at Respondent Meta (pending scheduled termination of employment on April 18, 2025). He is a resident of the state of Texas who has primarily worked for Meta out of his home in Texas and Meta's offices in Menlo Park, California and in London, United Kingdom ("U.K"). At all times relevant to this Complaint, Mr. Baig was a covered employee within the meaning of SOX.

3. Respondent 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.

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

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

6. Respondent Nitin Gupta is the current Vice President, Head of Engineering, WhatsApp at Meta.

7. Respondent Will Cathcart is the current Vice President, Head of WhatsApp at Meta.

8. Respondent Chris Cox is the current Chief Product Officer of Meta.

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

Jurisdiction

10. OSHA is responsible for receiving information about, investigating, and remedying violations of SOX and its implementing regulations and guidelines.

11. Mr. Baig and Respondent Meta entered into a tolling agreement dated May 6, 2023, in order to extend the deadline to file a complaint with 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. Mr. Baig filed a pre-termination complaint with OSHA on January

17, 2025. 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.

12. Mr. Baig received a notice of termination of employment due to poor performance on February 10, 2025. This new adverse action falls within the 180-day statute of limitations for claims under SOX.

Factual Allegations

13. Prior to Mr. Baig's joining the Company in January 2021, Meta, then known as Facebook, had already faced extensive scrutiny from federal agencies and the public concerning its security and data practices.

14. In 2011, the Federal Trade Commission ("FTC") announced a broad settlement with Meta that required Meta to respect the privacy wishes of its users and engage in regular privacy audits for 20 years. The eight-count FTC complaint that preceded the settlement alleged that Facebook had mishandled its users' personal information by making that information public, allowing advertisers to access personally identifiable user information, and sharing user information with outside application developers, contrary to Facebook's representations to its users.

15. As a result of the FTC's complaint, the FTC announced a proposed settlement with Facebook in 2011 – which the FTC officially approved in 2012 (2012 Privacy Order) – that required Facebook to "not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information," which included, inter alia, "(d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID or other persistent identifier; [or] (g) physical location." Moreover, it required Facebook to "establish and implement, and thereafter maintain, a comprehensive privacy

program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers, and (2) protect the privacy and confidentiality of covered information."

16. Just a few years later, however, Meta faced further public scrutiny over its handling of user data once again. In 2018, the FTC launched an investigation into Meta after public reporting revealed that political consulting firm Cambridge Analytica had improperly harvested and used the personal information of over 50 million users of its social media platform, Facebook.

17. Following a yearlong investigation by the FTC, in July 2019, the Department of Justice ("DOJ") filed a complaint on behalf of the FTC against Meta, alleging that Meta had violated its privacy promises to consumers and subsequently violated the 2012 Privacy Order and the Federal Trade Commission Act (FTC Act). Specifically, the DOJ alleged that Meta allowed third-party developers access to user data despite public announcements to the contrary. The DOJ also alleged that Meta did not maintain a reasonable privacy program that safeguarded the privacy, confidentiality, and Integrity of user information, as required by Part IV of the 2012 Privacy Order.

18. As a result of this complaint, the FTC and Meta entered into a modified privacy order ("2020 Privacy Order"), which the FTC announced in July 2019 and formally approved in August 2020. As part of this settlement, Facebook agreed to pay a $5 billion penalty, the largest-ever fine by the federal government against a technology company and almost 20 times greater than the largest privacy or data security penalty ever imposed worldwide.

19. Pursuant to the 2020 Privacy Order, the FTC required Meta to "restructure its approach to privacy from the corporate board-level down" and prohibited Meta from making

misrepresentations regarding the collection, use, or disclosure of certain user information. This "Covered Information" is defined in the 2020 Privacy Order as "information from or about an individual consumer" including but not limited to: first and last name; geolocation; mobile or telephone number; photos and videos; and IP address. The 2020 Privacy Order is in effect until 2040.

20. Importantly, the 2020 Privacy Order placed restrictions and imposed requirements not only on Meta as a whole, but also specifically on WhatsApp, especially as to how the entities collect and handle Covered Information. Under Part VII of the 2020 Privacy Order, Meta and WhatsApp were required to establish and maintain a "comprehensive privacy program" that "protects the privacy, confidentiality, and Integrity of the Covered Information collected, used, or shared by Respondent." The Order defined Integrity as "the protection of information from unauthorized destruction, corruption, or falsification." Moreover, the Order requires that Meta and WhatsApp:

a. Assess and document, at least once every twelve (12) months, internal and external risks in each area of its operation (*e.g.*, employee training and management; developer operations; partnerships with Covered Third Parties; sharing of Covered Information with Covered Third Parties or Meta-owned affiliates; product research, design, and development; and product marketing and implementation) to the privacy, confidentiality, or Integrity of Covered Information that could result in the unauthorized access, collection, use, destruction, or disclosure of such information; and

b. Design, implement, maintain, and document safeguards that control for the material internal and external risks identified by Respondent in response to Part

> VII.D. Each safeguard shall be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information.

21. The 2020 Privacy Order further stipulated that Meta and WhatsApp must have in place safeguards that include "designing, implementing, and maintaining access policies and controls that limit employee access to any table(s) or other comparable data storage units known to contain Covered Information to only those employees with a business need to access such Covered Information."

22. Moreover, under Part VII, the Order placed restrictions on WhatsApp's sharing of Covered Information with any other Meta affiliate: "Specifically with respect to Respondent's sharing of Covered Information with any other Facebook-owned affiliate, Respondent shall design, implement, maintain, and document safeguards that control for risks to the privacy, confidentiality, and Integrity of such Covered Information, based on the volume and sensitivity of such Covered Information that is at risk, and the likelihood that the risk could be realized and result in the unauthorized access, collection, use, destruction, or disclosure of the Covered Information."

23. At roughly the same time that the 2020 Privacy Order was announced, the Securities and Exchange Commission ("SEC") announced its settlement of charges against Meta for making misleading disclosures regarding the risk of misuse of Meta user data.

24. For over two years, Meta knew that third-party developer Cambridge Analytica had misused Facebook user data, yet Meta presented the risk of misuse of user data as merely

hypothetical in statements in SEC filings such as "our users' data may be improperly accessed, used or disclosed." To settle the charges, Meta agreed to pay $100 million.

25. WhatsApp, which Meta bought in 2014, also faced significant fines from regulatory bodies for its data practices. For instance, in September 2021, the Irish Data Privacy Commissioner ("IDPC") fined WhatsApp €225 million for issues related to WhatsApp's compliance with European Union General Data Protection Regulation ("GDRP") rules on data transparency in 2018.

26. This scrutiny continued into Mr. Baig's employment with Meta. In January 2023, the IDPC fined WhatsApp Ireland an additional €5.5 million for an issue involving misuse of data.

Mr. Baig, a cybersecurity and privacy expert, joined WhatsApp as its Head of Security, and he quickly discovered systemic cybersecurity problems.

27. Mr. Baig joined Meta with over 20 years of experience as a computer engineer and has specialized in cybersecurity for over 15 years. Prior to joining Facebook in 2021, Mr. Baig had led engineering teams and designed cybersecurity and data protection systems for companies such as PayPal, Capital One, Mastercard, and nextToken, including serving as Head of Security Architecture & Engineering at Capital One and Chief Technology Officer at nextToken. Mr. Baig also previously worked as a cybersecurity consultant for Amazon.

28. Based on this proven track record in privacy and cybersecurity, Meta recruited and hired Mr. Baig to be a Software Engineering Manager beginning in January 2021. It is a common practice for Meta to recruit external candidates several levels below their current designation and promote them quickly once they are inside Meta.

29. During Mr. Baig's five-week onboarding period in Meta "Bootcamp," Suren Verma, Head of Server Engineering at WhatsApp, persistently recruited him to join WhatsApp as its Head of Security. He began that role in February 2021.

30. In this role, which Mr. Baig currently holds (pending scheduled termination of employment on April 18, 2025), he is responsible for protecting WhatsApp users' and their data from data breaches, hackers, and other compromises.

31. Initially, Mr. Baig reported directly to Mr. Verma. In June 2021, however, Mr. Baig began reporting to Pinaki Mukerji, Head of Privacy Engineering. Despite reporting directly to Mr. Mukerji, Mr. Baig continued to have regular contact with Mr. Verma, who often preferred to meet directly with Mr. Baig.

32. Shortly after joining WhatsApp, Mr. Baig learnt that WhatsApp previously didn't have a cybersecurity team, and it was created in response to the 2019 Pegasus attack on WhatsApp users. Mr. Baig learnt that his predecessor and the security team were working on preventing "stanzaming attacks," a term which Mr. Baig was unfamiliar with despite his 15 plus years of experience in cybersecurity.

33. This puzzled Mr. Baig, and he kept asking questions. A few weeks later, he understood that the entire security team was working on mitigating buffer overflow and/or remote code execution attacks in the C/C++ code of the WhatsApp application. They primarily focused on fuzzing approximately 20,000 C/C++ functions to find remote code execution vulnerabilities.

34. Mr. Baig also learnt that WhatsApp collected significantly more user data than Signal, another messaging application. Among other things, WhatsApp collects and stores users' address book, group membership, last seen status, profile photo, etc.

35. This further surprised Mr. Baig, as WhatsApp, which is known for its strong security brand externally, had such a small security team of just 6 engineers, and they were all only working on this tiny aspect of application security. All the other teams in WhatsApp were well staffed. The engineering team had about 1200 engineers. In addition, there were about 100 product managers, about 100 product designers, nearly 200 data scientists, etc. WhatsApp overall had about 3000 employees.

36. Mr. Baig spent his initial six months at the Company onboarding, learning about the Company, and ensuring that the projects that had been in progress when he joined successfully continued.

37. Mr. Baig's successful transition into his role was acknowledged in his first performance review that he received in August 2021. Mr. Baig received a "Meets All Expectations" rating, with no areas of improvement listed. In the meeting, Mr. Mukerji told Mr. Baig it was standard practice that, for an employee's first rating cycle, the employee would receive either a "Meets All" or a "Meets Most" rating.

38. Mr. Baig, however, soon learned that WhatsApp's cybersecurity posture had serious deficiencies. In September 2021, Mr. Baig conducted a "Red Team Exercise" – a simulation of a cybersecurity attack to reveal vulnerabilities – with the help of Meta's Central Security team (later known as the "X-Sec team" after internal rebrands), which is responsible for providing tooling (both hardware and software) and security consulting support to all of Meta, including WhatsApp.

39. This exercise revealed that any WhatsApp engineer with production access – roughly 1,500 engineers – could move or steal WhatsApp user data, such as users' address book

with friends' contact information, without a trace. Mr. Baig shared this concerning finding with Mr. Verma in verbal conversations.

40. Mr. Baig and the Central Security team published a report about the red team findings in an internal forum named REDACTED Group. This group has on average about 1700 WhatsApp employees, primarily engineers and engineering leaders including Mr. Verma and Nitin Gupta, Vice President, Head of Engineering, WhatsApp, whom Mr. Verma reported into.

41. Given this finding and other indications Mr. Baig had begun to observe that the WhatsApp cybersecurity posture had significant problems. Mr. Baig thought it was critical to figure out if WhatsApp knew the basic information necessary for a functioning cybersecurity program: (1) what user data it was collecting; (2) where and how it was storing the data; and (3) who had access to it.

42. On about five occasions between September 2021 and September 2022, Mr. Baig raised his concerns with Mr. Verma that WhatsApp needed to determine if it had this basic information, but Mr. Verma ignored him. Instead, Mr. Verma directed Mr. Baig to do what his predecessor had done, which was work on application security, write "fuzzers" (a software testing method intended to reveal software defects and vulnerabilities), and spend his time on other, less strategically oriented projects.

43. WhatsApp's cybersecurity posture was made even worse by the fact that the Company refused to allocate more than around 10 engineers to the Security team at any point, despite WhatsApp having about 1,200 engineers in total. This lack of staff meant that Mr. Baig was unable to take proactive, big picture action to remedy the systemic cybersecurity vulnerabilities.

44. Making the matter worse, WhatsApp's performance and reward structure for engineers internally referred to as Performance Summary Cycle ("PSC") incentivized engineers to do busy work by writing large number of lines of code in order to keep the WhatsApp site and mobile app functioning, so the engineers in WhatsApp were disincentivized from working on these systemic cybersecurity issues that were not solved by writing large number of lines of code and did not relate to the WhatsApp site and mobile app functioning.

45. In addition, the PSC culture rewarded engineers for making things artificially complex. For the most part, engineers and product managers copied features from Signal, Telegram, iMessage, etc. and created busy work for themselves to meet the PSC expectations:

a. WhatsApp Server engineers would misconfigure and reconfigure the site thousands of times per year to meet the PSC expectations. This was the only way for them to get promoted or to justify their seniority.

46. Unlike the other whistleblower allegations where Meta is accused of "prioritizing profits over user safety," Mr. Baig quickly learnt that WhatsApp was not making a profit and in fact it was losing billions of dollars every year:

a. The cost of WhatsApp's acquisition to Meta's shareholders in today's money would be around $200 billion, if we factor in Meta's current stock price vs Meta's stock price when WhatsApp was acquired in 2014.

b. WhatsApp currently loses between $[REDACTED] billion per year and the way WhatsApp calculates revenue internally is questionable e.g.: If a business chooses to advertise on Facebook or Instagram and chooses to be contacted by its customers on WhatsApp instead of a phone call or over email, it is considered as WhatsApp revenue.

c. Mr. Baig understood that given the incentive model, WhatsApp would probably never make a profit unless it chooses to use the social graph, which is users' address book, group memberships, etc. and target advertisements using this data on Facebook, Instagram, Threads, etc. Another way WhatsApp could make a profit is by copying a successful future business model of other messaging applications.

d. Mr. Baig also learnt that in the case of WhatsApp, it was not profits that are prioritized over user safety, but the PSC culture and user growth metrics.

47. Despite Mr. Verma's refusal to engage on protecting user data and the staffing challenges, in February 2022, Mr. Baig created a product requirements document for the Privacy Infra team to build a comprehensive data classification and a data handling system. This was the first step in figuring out what user data WhatsApp had collected, where it was stored, and who has access to it.

48. The Privacy Infra team prioritized other projects, and when Mr. Baig raised this issue to Mr. Mukerji, Mr. Mukerji supported the Privacy Infra team's prioritization of those other projects.

49. In the spring of 2022, an internal audit initiated by Meta's Board found that the unmonitored production access engineers had posed a "high risk" to WhatsApp infrastructure because such access could result in the WhatsApp site being brought down. The cause of this serious vulnerability had the same root cause as the user data privacy concerns that Mr. Baig had raised in September 2021 after the red team exercise.

50. Mr. Baig and his team proposed two solutions – instituting an immutable audit trail of all actions taken by engineers and filtering out harmful computer commands that could

allow engineers to bring down the WhatsApp site. The server engineering Director, Dick Brouwer to whom Mr. Verma delegated the audit did not commit to implementing the solution until the auditors escalated the audit item to their manager, Charu Chandra, Director, Technology Infrastructure Audit.

51. Even while he repeatedly raised his concerns that WhatsApp had systemic cybersecurity problems to Mr. Verma and Mr. Mukerji, Mr. Baig continued to receive positive feedback and assessments.

52. In February 2022, Mr. Baig received a performance rating of "Exceeded Expectations," and his managers discussed with him the possibility of him receiving a promotion in the next six to twelve months. In the write-up Mr. Mukerji provided as part of Mr. Baig's performance review, Mr. Mukerji wrote, among other positive statements, that "Attaullah demonstrated deep security skill and product centric thinking," and "Attaullah and security team made great progress on multiple 'understand' projects despite little help/engagement initially from Product Management."

53. Notably, Mr. Mukerji rated Mr. Baig an Exceeded Expectations in "People Management" and a "Meets All" in Collaboration. On the basis of this positive performance review, Mr. Mukerji's performance summary cycle letter stated, "Based on your accomplishments and the results that you delivered in H2 2021, your performance assessment is exceeds expectations. This means that during that time, you consistently exceeded the high expectations at your level across all your responsibilities and produced results that set an example for those around you. You consistently exhibited very strong performance."

54. Accordingly, Meta awarded Mr. Baig a 6.13% increase in total cash compensation, *i.e.*, salary plus bonus incentive. Moreover, Meta also awarded Mr. Baig an

"equity refresher grant" of 1,283 restricted stock units (RSUs), which were worth $293,178 at the time and would vest in 1/16th of these RSUs on each quarterly vest date beginning May 15, 2022.

55. At the beginning of 2022, Meta switched from a semi-annual to a yearly performance cycle. Accordingly, instead of a full performance assessment, in July 2022, Mr. Baig had a "Touchpoint feedback session," a half yearly check-in and feedback session, albeit less formal than the annual PSC review. This midyear review was positive and focused mostly on Mr. Baig's growth and trajectory towards promotion to the next level during the next full performance review in February 2023.

56. In this Touchpoint, Mr. Mukerji also shared with Mr. Baig that he had put Mr. Baig's name up for promotion and reviewed Mr. Baig's "Growth Plan" with other engineering leaders. "Growth Plan Reviews" are a term of art at Meta and are meant for employees who are ready to be promoted in the next three to six months.

Beginning in the summer of 2022, Mr. Baig reported WhatsApp's systemic cybersecurity failures to WhatsApp's leadership.

57. In summer of 2022, there were two cybersecurity incidents that impacted WhatsApp: The first involved a messaging app called HeyMods that impacted WhatsApp users, and the second was a data breach at Twilio, a company that partners with WhatsApp, that impacted a limited number of WhatsApp users.

58. In the aftermath of these security incidents, on August 18, 2022, Mr. Baig met with Will Cathcart, Vice President, Head of WhatsApp, WhatsApp, Vice President of Global Communications Carl Woog, Director & Associate General Counsel Jessica Romero, and Associate General Counsel Brady Freeman. In this meeting, Mr. Baig briefly talked about

WhatsApp's systemic cybersecurity deficiencies, raising the concerns he had been raising with Mr. Verma and Mr. Mukerji for nearly a year.

59. Specifically, Mr. Baig told Mr. Cathcart that WhatsApp security was dangerously understaffed – it had about ten engineers working on security, while a comparably sized company had around 200 – and WhatsApp was not focusing on systemic security issues. At the end of the meeting, Mr. Cathcart asked Mr. Baig to create a report on how WhatsApp can respond to such cybersecurity threats and incidents for a follow-up meeting with the same group.

60. The follow-up meeting was initially scheduled for September 8, 2022. In preparation for this meeting, Mr. Baig prepared a pre-read document for the above group that detailed WhatsApp's systemic cybersecurity failings. Since Mr. Verma and Mr. Mukerji were not going to attend the meeting, they did not receive the pre-read.

61. Although the content of WhatsApp messages is secure and encrypted, WhatsApp was failing to protect and secure a host of other user data elements, including users' profile photos, phone numbers, friends' phone numbers and other contact information, IP address, and the data concerning the last time at which a user logged in. In drafting the pre-read and preparing for the meeting, Mr. Baig identified six critical issues concerning this data:

a. WhatsApp does not know what user data it is collecting: WhatsApp does not have a comprehensive list of all user data elements which WhatsApp collects. Mr. Baig understood that laws such as the California Consumer Privacy Act ("CCPA") and the European Union's GDPR require WhatsApp to know and disclose which user data elements WhatsApp collects. Additionally, since WhatsApp did not know what data, it is collecting, it could not have a successful privacy program, as required by the 2020 Privacy Order, because WhatsApp

could not protect data or honor its user agreements without knowing which data it collects and for what business purpose.

b. WhatsApp does not know where it stores the user data it collects: WhatsApp does not have a comprehensive inventory of all systems where it stores user data. Lack of a clear data inventory increases the risk of data breach because the Company does not know what user data elements to protect or how to do so. This failure also prevents WhatsApp from properly disclosing to regulators and users the data it collects.

c. WhatsApp allowed roughly 1,500 engineers – including all WhatsApp engineers and even some Meta engineers – to access user data without restriction, including information that qualifies as Covered Information under the 2020 Privacy Order. The FTC order required WhatsApp to design, implement, maintain, and document safeguards that (1) limit employee access to Covered Information to only those employees with a business need to access Covered Information and (2) control for risks to the privacy, confidentiality, and Integrity of Covered Information with respect to WhatsApp's sharing of Covered Information with other Facebook-owned affiliates. There was no business need for all WhatsApp engineers to have unfettered access to all Covered Information, nor were there any controls in place that Mr. Baig was aware with respect to the access that the Meta engineers had to Covered Information. To paint the gravity of the vulnerability that this places users in, any one of these roughly 1,500 engineers could find and identify an elected official's geographic location while messaging (through their IP address) and see the contact number of who they were messaging.

d. WhatsApp does not know who has accessed user data: WhatsApp does not have a monitoring system in place for user data access. This means that WhatsApp cannot tell if someone is accessing user data in a suspicious way, and it does not have a process to audit access. This failure compromises user data security. Because WhatsApp cannot monitor employee access, it cannot identify and react to suspicious or improper activity. This inability means that WhatsApp is not meeting its obligation under the 2020 Order to have a "comprehensive privacy program (Privacy Program) that protects the privacy, confidentiality, and Integrity of the Covered Information collected, used, or shared by Respondent."

e. WhatsApp cannot discover a data breach even after it has happened. While companies commensurate to WhatsApp's and Meta's size have a 24-hour Security Operations Center ("SOC") to detect and respond to anomalous data access, including data breaches, in real time, WhatsApp and Meta lacked, and continue to lack, such an ability. This organizational failure means that WhatsApp and Meta do not know, and hence cannot respond to, data breaches as they occur. The FTC privacy order required Meta to "implement, and thereafter maintain, a comprehensive information security program that is designed to protect the security of Covered Information" and that contains "safeguards appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the Covered Information." Because a SOC is appropriate for a company of WhatsApp's and Meta's size and complexity and necessary for identifying and responding to data breaches – companies similar in size to Meta such as Amazon, Apple, and Google have one, while companies the

size of WhatsApp, such as Indeed, PayPal, and Robinhood also have one – WhatsApp's organizational structure raises compliance issues with the 2020 Privacy Order.

f. Around 100,000 WhatsApp users per day have their accounts compromised – often someone taking over and locking the user out of their account, where they can access Covered Information including photos, groups, phone numbers, contact information, and private messages – but WhatsApp had failed to take adequate action to address this extensive issue.

62. In the pre-read, Mr. Baig not only raised these issues but also identified that he believed they rose to the level of potential violations of Meta's legal obligations. For instance, he expressly referred to the SEC and FTC settlements in 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."

63. On September 8, 2022, ahead of the meeting, Mr. Baig shared the pre-read with the attendees, including Mr. Cathcart. After Mr. Cathcart reviewed the pre-read, he decided to postpone the meeting and to include members of Mr. Baig's management chain in the meeting.

64. In response to news that the meeting was postponed and that his supervisors would now be attending the meeting, Mr. Baig wrote to Mr. Cathcart on WhatsApp expressing concern to Mr. Cathcart that he did not want his managers to feel like he went around them and escalated the failures directly to Mr. Cathcart. He also told Mr. Cathcart that he feared his managers would retaliate against him for reporting these problems to Mr. Cathcart.

65. Mr. Baig feared this retaliation because his managers had ignored the systemic cybersecurity problems for years, which had resulted in the current appalling state of

WhatsApp's cybersecurity. In response, Mr. Cathcart told Mr. Baig to proceed nonetheless and inform his managers that he had prepared the report at Mr. Cathcart's request.

Mr. Baig immediately began experiencing retaliation because of his cybersecurity report.

66. The new meeting was scheduled for September 30, 2022, and it included Mr. Verma as well as Mr. Gupta. In preparation for the meeting, Mr. Verma reviewed Mr. Baig's pre-read for the meeting on September 26, 2022. Mr. Verma immediately contacted Mr. Baig to inform Mr. Baig that he was extremely unhappy about the report.

67. During their conversation on a video call over WhatsApp, Mr. Verma made clear that he was upset about the content of the pre-read and that Mr. Baig would suffer retaliation for the report. Specifically, Mr. Verma told Mr. Baig that it was "the worst doc I have seen in my life" and asked Mr. Baig if he was "going to tell Will [Cathcart] that the whole system is broken?". He then told Mr. Baig that Mr. Gupta would fire him for writing a document like this.

68. Mr. Verma also warned Mr. Baig that Mr. Verma had been working on ensuring that Mr. Baig and his team receive a good compensation package including discretionary equity in the upcoming review cycle, and that this document really upset Mr. Verma. Mr. Baig understood Mr. Verma's statement as a not-too-subtle threat.

69. Mr. Verma's threats immediately became reality. Within days, Mr. Baig began to experience retaliation. Prior to this incident, Mr. Verma on multiple occasions had told Mr. Baig that, given Mr. Baig's rare and critical skillset in cybersecurity, Mr. Baig can grow to the highest levels in Meta very quickly.

70. On September 29, 2022, Mr. Baig received negative feedback about his performance for the first time. Mr. Mukerji told Mr. Baig that he was not performing well, and that the quality of his written work product was insufficient. This feedback was the opposite of

the feedback Mr. Baig had received for the prior year and a half, including in June, when Mr. Mukerji had lauded Mr. Baig's "[e]xtreme focus and clarity on project scope, timeline etc." Mr. Baig later learned that Mr. Mukerji had also marked Mr. Baig as "Needs Support" on or before September 30, 2022, for the October 2022 Touchpoint.

71. In response to Mr. Verma's retaliation, Mr. Baig initially tried to take steps to placate Mr. Verma. After Mr. Verma's angry feedback, Mr. Baig backed away from a systematic diagnosis of WhatsApp's cybersecurity deficiencies.

72. However, on September 30, 2022, when Mr. Baig shared this curtailed document with Mr. Cathcart, Mr. Cathcart cancelled the scheduled follow-up meeting and directed Mr. Baig to return the document's focus to systematic issues.

73. Meanwhile, Mr. Mukerji's new hostility towards Mr. Baig continued. He began questioning and micromanaging Mr. Baig and his work by creating artificial work and conflicts, looking for situations to show Mr. Baig "Needs Support," and actively soliciting negative feedback on Mr. Baig from Mr. Baig's peers.

74. Previously, Mr. Mukerji had generally not been involved in Mr. Baig's work and almost never reviewed any documents he produced. Now, however, Mr. Mukerji began insisting on reviewing all of Mr. Baig's work product and setting up a series of meetings – about two to three meetings a week – that he required Mr. Baig to attend in which Mr. Mukerji critiqued Mr. Baig's work and added numerous comments to his work product. Mr. Mukerji sent Mr. Baig harsh and negative messages, such as one on October 6, 2022, that read, "I am questioning your judgment call."

75. This sudden shift in feedback and treatment came as a shock to Mr. Baig and contrasted starkly with the glowing performance reviews he received prior to his sharing of the pre-read with his managers.

76. In response to Mr. Mukerji's and Mr. Verma's treatment, Mr. Baig raised his concerns about retaliation in a prescheduled call with Lauren Yoon, the Human Resources Business Partner ("HRBP") assigned to him. On September 29, 2022, Mr. Baig spoke briefly with Ms. Yoon about the treatment he was experiencing. Mr. Baig informed Ms. Yoon that he was afraid that Mr. Verma and Mr. Mukerji were retaliating against him because of the pre-read. Ms. Yoon told Mr. Baig that she needed time to think the situation through. In this meeting Mr. Baig, shared the quote from Mr. Verma about "the whole system being broken". Ms. Yoon swiftly agreed that in fact "the whole system is broken".

77. Over the course of the next weeks, Ms. Yoon pinged Mr. Baig on multiple occasions for a follow up. Mr. Baig responded and set up a meeting for the next week.

78. Mr. Verma mirrored Mr. Mukerji's treatment of Mr. Baig. To try to resolve the increasing tension, Mr. Baig reached out to Mr. Verma.

79. On October 6, 2022, Mr. Baig met with Mr. Verma. For the first time since Mr. Baig joined Meta, Mr. Verma told Mr. Baig that he was not meeting expectations and needed additional support because Mr. Mukerji had been spending significant time with Mr. Baig to "support" him. "Needs Support" is a term of art at Meta and indicates that a manager is spending too much time with an employee. It can also have dramatic implications for the employee.

80. In response to this ongoing retaliation, on October 7, 2022, Mr. Baig met with Ms. Yoon on a video call. During that meeting, Mr. Baig explained to Ms. Yoon that although

he had a great working relationship with both Mr. Mukerji and Mr. Verma before the pre-read, he had noticed a shift in how they were treating him immediately following Mr. Baig's raising of cybersecurity concerns.

81. Ms. Yoon told Mr. Baig that she would have included Mr. Verma in the creation of the report, even though Mr. Cathcart had expressly told Mr. Baig not to do so. She advised Mr. Baig to speak with Mr. Verma directly about the issue.

82. Ms. Yoon incorrectly told Mr. Baig that Mr. Verma and Mr. Mukerji were not retaliating against Mr. Baig in a legal sense because there was not a "protected category" at issue, by which she meant discrimination or retaliation based on Mr. Baig's membership in a protected class. Mr. Baig told Ms. Yoon that he would soon share a written report on this. On October 10, 2022, Mr. Baig began writing a retaliation report.

83. On October 17, 2022, Mr. Mukerji had a Touchpoint feedback conversation with Mr. Baig. During the roughly thirty-minute meeting, Mr. Mukerji repeatedly told Mr. Baig that he was in "Needs Support" territory and required additional support. Mr. Mukerji told Mr. Baig that Mr. Baig needed to secure positive feedback from two teams, Integrity and Data Science, by the end of the year, or his yearly PSC rating would be negatively affected.

84. This feedback alarmed Mr. Baig, as he had received an "Exceeds Expectations" rating on the prior year's performance review and Mr. Mukerji was working on Mr. Baig's promotion in upcoming PSC cycle in February 2023. After the meeting, Mr. Baig had asked Mr. Mukerji and Mr. Verma to help define the accountability model they wanted him to achieve with the Integrity team, but both managers only gave vague, non-actionable feedback, such criticizing Mr. Baig for not collaborating well enough.

Mr. Baig again reported to WhatsApp leadership the systemic cybersecurity failures and faces additional retaliation.

85. Despite this ongoing retaliation, on October 18, 2022, after over a month and a half of delay, Mr. Baig gave the presentation to Mr. Cathcart, Mr. Verma, Mr. Gupta and other WhatsApp Vice Presidents and leadership, roughly ten people in total.

86. In the pre-read document which Mr. Baig drafted, Wael Salloum, Head of Data Science, WhatsApp, added a comment, requesting the entire document to be marked as attorney-client privileged, even though the purpose of the document was not to seek legal advice and Mr. Baig was not instructed to draft it by an attorney. Mr. Salloum clearly understood the gravity of the cybersecurity concerns raised by Mr. Baig.

87. Mr. Gupta also added a comment in the pre-read document. The comment read "ouch! Did we check with Meta security as to what is their own assessment of their situation" implying it hurts to hear about the cybersecurity gaps because it makes others look like they do not know what they are doing. This set the tone for the rest of the retaliation and the inaction to fix the cybersecurity gaps required under the 2020 Privacy Order.

88. As per Mr. Baig's observation, 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(s) who is raising the concern.

89. At the beginning of the meeting, Mr. Cathcart opened the discussion by telling everyone not to blame Mr. Baig for the report and that Mr. Cathcart took responsibility for the report because Mr. Cathcart had requested that Mr. Baig create it.

90. The meeting was relatively short because much of the commentary had occurred prior to the meeting through comments on the pre-read that Mr. Baig had prepared and circulated

to the group. During the meeting, Mr. Baig said that if WhatsApp did not overhaul its cybersecurity posture, WhatsApp would get sued because of a data breach.

91. At another point during the meeting, Head of WhatsApp Global Public Policy Jonathan Lee, asked, "Are we going to be in the same situation as Mudge at Twitter?". Mr. Lee's question made clear that WhatsApp leaders understood that the cybersecurity problems that Mr. Baig was raising were very serious and implicated Meta's legal and regulatory obligations.

92. By that time, it had been reported that the Twitter whistleblower disclosures had resulted in a Congressional investigation into Twitter and lawmakers encouraging the FTC to investigate Twitter for potential violations of Twitter's FTC consent order regarding data privacy.

93. Mr. Baig also specifically raised his concern that WhatsApp branded itself as secure, yet he knew that WhatsApp had systemic cybersecurity failures that made it fundamentally unsecure. In response, Mr. Woog said that because security is WhatsApp's brand, the issues Mr. Baig raised scared him and called the document a "foundational doc." Notably, during the meeting, Mr. Verma was visibly angry during the conversation. He was very agitated and was outwardly hostile to Mr. Baig for raising these issues.

94. At the end of the meeting, Mr. Cathcart directed Mr. Verma to address the systemic cybersecurity problems that Mr. Baig had identified. Mr. Cathcart told Mr. Verma to fix the issues, talk to Meta's Central Security team, and have a follow-up meeting. However, even months or years later, there has been no follow-up meeting with the same group, and Mr. Verma did not address the cybersecurity issues that Mr. Baig identified.

95. After the meeting, Mr. Baig followed up by sending an email to all the invitees, including Mr. Cathcart, in which he included a link to coverage by Forbes of Peiter Zatko and the cybersecurity vulnerabilities he had revealed at Twitter. The topline of the Forbes article that Mr. Baig shared stated, "Twitter's former head of cybersecurity accused the social media company of committing fraud and numerous 'egregious' security violations in an explosive whistleblower complaint revealed Tuesday, shaking confidence in the much-maligned platform and sending its stock spiraling." By sharing this article, Mr. Baig made crystal clear that the issues he was raising were about potential legal violations.

96. It is important to note that after this meeting Mr. Cathcart till February 10, 2025, did not review any of the cybersecurity projects that Mr. Baig's team worked on. Mr. Cathcart on average reviewed about ten projects per week from various teams across WhatsApp. In other words, Mr. Cathcart distanced himself from the glaring cybersecurity and privacy gaps while he continued certifying WhatsApp's compliance with the 2020 Privacy Order. Mr. Cathcart also did not escalate the cybersecurity gaps to the Audit & Risk Oversight Committee ("AROC") in Meta's Board of Directors.

97. The day after the meeting, on October 19, 2022, Mr. Baig filed a formal report of retaliation with Ms. Yoon. Mr. Baig had held off on filing a formal retaliation report since early October 2022 because he had previously had a close relationship with Mr. Verma, considered them to be friends, and wanted to see if their relationship could be repaired. However, once Mr. Mukerji told Mr. Baig that he was in "Needs Support" territory during the October 17, 2022, Touchpoint, Mr. Baig realized that the retaliation he was facing was ongoing and likely to continue.

98. In this complaint, Mr. Baig documented the retaliation he was facing from Mr. Verma and Mr. Mukerji after he circulated his pre-read on September 26, 2022. Mr. Baig described a "sudden shift in conversations" and detailed the conduct described above. In this retaliation report, Mr. Baig reported these developments to Ms. Yoon, "I feel that [I] am being deliberately setup to fail" because of his creation of the pre-read.

99. In this complaint, Mr. Baig also documented a sudden shift in how Mark Tsimelzon, Director of Engineering, WhatsApp, started treating Mr. Baig immediately after the pre-read. Mr. Tsimelzon was helping Mr. Baig by unblocking his project and suddenly Mr. Tsimelzon started telling Mr. Baig that the issues he was bringing up are non-issues and Mr. Tsimelzon will not help Mr. Baig. Earlier on June 15, 2022, Mr. Tsimelzon had shared positive peer feedback on Mr. Baig in the performance management tool, which included this quote "I want to help him personally to be as successful as he can be." Despite Mr. Baig's well-documented allegations, Ms. Yoon never acknowledged the complaint, nor did she reach out to Mr. Baig to interview him. To Mr. Baig's knowledge, there was no investigation carried out at this time, although Ms. Yoon occasionally messaged Mr. Baig to see how he was doing.

100. In the aftermath of the October 18, 2022, meeting, Mr. Mukerji continued to micromanage Mr. Baig by sending him a flood of messages daily and arranging for frequent meetings. Although Mr. Mukerji generally had not reviewed Mr. Baig's work before October 2022, he now insisted on reviewing nearly all of it.

101. Around this time, Mr. Baig raised a concern about Mr. Tsimelzon's team measuring their own success with respect to Account Takeover ("ATO"), Scraping, Impersonations, and other user related harms. Mr. Baig noticed that they were manipulating user harm metrics at the beginning and end of every PSC cycle to get better performance ratings. Mr.

Salloum agreed with Mr. Baig and echoed similar concerns. Shortly thereafter Mr. Salloum left Meta under suspicious circumstances.

102. During Mr. Baig's tenure, none of the user harm metrics from Mr. Tsimelzon's team were independently audited, despite Mr. Baig raising concerns numerous times. In other words. Meta and WhatsApp leadership allowed this to go unchecked as they were focused primarily on WhatsApp user growth metrics.

103. On November 14, 2022, Mr. Mukerji and Mr. Verma met with Mr. Baig and presented him with a verbal warning. Mr. Mukerji and Mr. Verma claimed that Mr. Baig had violated Meta's Respectful Communication Policy through "unprofessional and disrespectful" interactions with the Integrity, WhatsApp Payments, and Data Science teams. They alluded to "several instances where word choice, tone or volume of voice, and dismissive and/or belittling behavior has occurred."

104. Additionally, they claimed that they had discussed these thematic concerns during one-on-one meetings, touchpoint feedback, and async but that Mr. Baig had failed to internalize and act on the feedback. Mr. Mukerji and Mr. Verma refused to give Mr. Baig any specifics – claiming instead that everything is confidential – and instructed Mr. Baig not to try to find out any more detail. They told Mr. Baig that he was expected to review the Respectful Communication Policy and inquire about Emotional Intelligence training for managers. They warned Mr. Baig that any further conduct could result in further discipline. They followed up with a documented summary of the conversation.

105. During the discussion Mr. Verma and Mr. Mukerji reprimanded Mr. Baig about a question that Mr. Baig had asked the payments team during a cybersecurity risk assessment. At the end of the risk assessment Mr. Baig had asked the payments team "Do you understand the

risks here?". In Mr. Baig's experience, this is a completely normal question to ask during a cybersecurity risk assessment.

106. The next day, on November 15, 2022, Mr. Baig replied via email and stated that while he appreciated this feedback, he had concerns "with the lack of clarity and accuracy of some of the things mentioned here." Mr. Baig wrote that he was hearing the allegations of unprofessional and disrespectful conduct for the first time, contrary to their claim that the thematic concerns had been discussed during one-on-one meetings, touchpoint feedback, and async. Mr. Baig cited to his prior evaluations, which contained no mention of any such problems or any violation of any company policy. To the contrary, Mr. Baig had received positive reviews on his collaboration and communication earlier that year.

107. Mr. Baig reached out to Employee Relations Business Partner ("ERBP") Mona Sawani about the feedback. During a video call, without prompting from Mr. Baig, Ms. Sawani acknowledged that there were two problems with the verbal warning:

a. First, the feedback Mr. Verma and Mr. Mukerji provided was generic and not actionable, which Ms. Sawani told Mr. Verma and Mr. Mukerji before they gave Mr. Baig the verbal warning, yet they issued the warning despite her feedback.

b. Second, Ms. Sawani raised concerns about the unusual timing of the complaint that had led to the verbal warning. While the complaint alleged that Mr. Baig's problematic conduct had begun in July 2022, it was not filed until October 2022. Ms. Sawani expressed concern about why the complaint had been filed unusually late.

108. Despite these problems with the complaint and verbal warning, Mr. Baig subsequently learned that Meta had considered terminating his employment.

109. Sometime later, Mr. Baig learnt that Ms. Sawani was no longer employed at Meta and was potentially impacted by the layoffs.

110. In the aftermath of the verbal complaint, Mr. Baig endeavored to take all the steps possible to address the issues raised. He reviewed the Respectful Communication Policy and scheduled an Emotional Intelligence Training for managers, although Meta subsequently cancelled the training, and Mr. Baig remains on a waitlist for the rescheduled training.

111. Over the subsequent months, however, Mr. Mukerji and Mr. Verma continued to micromanage Mr. Baig's work rather than addressing the cybersecurity issues Mr. Baig had identified.

112. Additionally, as Mr. Verma had threatened in late September 2022, he and Mr. Mukerji attempted to interfere with Mr. Baig's ability to reward the work of his subordinates on the Security team with adequate compensation and promotions. First, Mr. Mukerji did not support a Security team member getting a promotion they deserved. Second, Mr. Mukerji met with the Security team and told them that they were not doing their job well, without citing to any specific basis for that assessment. In response to Mr. Mukerji's treatment, two people left the team. Employees on the Security team expressed frustration to Mr. Baig with Mr. Mukerji's retaliation.

113. Because Mr. Mukerji exercised such control over Mr. Baig's team members' ratings, on or around January 13, 2023, Mr. Baig spoke with Mr. Gupta to resolve the issue. After Mr. Baig provided Mr. Gupta with a written document supporting his concerns about Mr. Mukerji's conduct towards his subordinates, Mr. Gupta ensured that the Security team received the promotions, ratings, and compensation they deserved.

114. Given the hostility that Mr. Baig was facing, he sought PSC feedback from supporters which included Mr. Woog. To Mr. Baig's surprise, Mr. Woog submitted very negative feedback and blamed Mr. Woog's external communication failures on Mr. Baig. Mr. Baig sought friendly non-legal advice from Ms. Romero about Mr. Woog's feedback. Ms. Romero was equally surprised as Mr. Woog had shared very positive feedback about Mr. Baig with Ms. Romero and others earlier. Ms. Romero referred to Mr. Woog as being "a snake."

Mr. Baig received a retaliatory performance review resulting in significant lost compensation, as well as a lost promotion opportunity.

115. Following Mr. Baig's escalation of the compensation issue to Mr. Gupta, Mr. Baig believed that the retaliation he was facing might subside.

116. On January 31, 2023, February 7, 2023, and February 14, 2023, Mr. Baig had meetings with Mr. Mukerji where Mr. Mukerji told Mr. Baig that his performance was perfect except for the collaboration issue. Mr. Mukerji added that Mr. Baig will receive a "Greatly Exceeds Expectations" or even a "Redefines Expectations" rating if he can sort the collaboration issues out and said he was getting Mr. Baig a mentor so Mr. Baig could work to receive a high rating and promotion.

117. On February 24, 2023, Mr. Baig had his annual PSC performance review. Mr. Baig received a "Consistently Meets Expectations." This rating was one step down from the prior year's "Exceeds Expectations."

118. During his performance review meeting, Mr. Mukerji claimed that the poor collaboration rating stemmed from the complaint that someone had made against Mr. Baig in October 2022, and had been the basis on which Mr. Mukerji and Mr. Verma had lowered Mr.

Baig's performance rating. While Mr. Baig received almost forty pages of peer feedback, Mr. Mukerji cherrypicked the few examples of negative feedback.

119. Additionally, although a "Consistently Meets Expectations" is nominally an average rating, Mr. Baig's supervisors included very negative comments in the "Areas of Improvement" section. Managers doing PSC reviews need to specifically choose to add the "Areas of Improvement" section, and Mr. Baig had never received similar negative feedback in his performance reviews.

120. On March 3, 2023, Mr. Verma met with Mr. Baig to discuss his rating with him. Mr. Verma informed him 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 than Mr. Baig received.

121. Mr. Verma also voluntarily acknowledged that Mr. Salloum had asked him not to give Mr. Baig the verbal warning on November 14, 2022, as the person in Data Science in Mr. Salloum's team, who complained about Mr. Baig was having collaboration issues with several other people at Meta.

122. Mr. Verma, however, also told Mr. Baig that they had contemplated terminating Mr. Baig in November 2022 instead of giving him a verbal warning. Mr. Verma then warned Mr. Baig that he would be terminated if there were another incident. Mr. Verma also enquired with Mr. Baig to see, if Mr. Baig will voluntarily leave Meta because of this review.

123. Mr. Baig's lower rating significantly impacted his promotion prospects and compensation. Because of the review, Mr. Baig did not receive the promotion he had deserved. Had Mr. Baig received a "Greatly Exceeds Expectations" rating or higher, as he should have,

Mr. Baig would have received roughly at least $1 million more in total compensation, a figure that includes a higher bonus, formulaic equity grant, and a discretionary equity grant but does not include the increase in compensation that would have accrued from a promotion. A promotion would have likely included around $40-45,000 in additional base salary, an increase in yearly bonus given the higher compensation, and new additional RSUs worth at least $200,000 at the time.

124. The discretionary equity grant would have been in the ballpark of at least $600,000 value. This discretionary equity grant is not tied to overall performance rating and is instead tied exclusively to "Impact," meaning that Mr. Baig's managers could have given him this equity grant even with his rating at "Consistently Meets Expectations."

125. However, Mr. Verma and Mr. Gupta decided not to award Mr. Baig this significant grant, even though they acknowledged in his performance review that he solved problems that many people thought could not be solved, he made "a number of contribution[s]" under "Org Impact," and had "unblocked the team" on several projects.

126. In addition to taking on a manager's responsibilities, Mr. Baig also played the role of an individual contributor product manager and a senior technical lead. An employee of Mr. Baig's experience, who had made the kind of impact acknowledged in the PSC review, should have received the discretionary equity grant.

127. Just before and after the negative performance review, Mr. Baig continued to face retaliation. Mr. Mukerji continued to manage Mr. Baig in a manner clearly designed to portray Mr. Baig as being incompetent and needing more support, setting him up for further negative feedback, placement on a Performance Improvement Plan, and potential termination.

128. For example, in late February 2023, Mr. Mukerji created fake work by asking Mr. Baig to recreate a document which had already been widely reviewed and then made close to fifty comments on the one-page document that he directed Mr. Baig to draft. Mr. Mukerji used this document to claim that he was coaching Mr. Baig to help him develop communication skills.

129. In February 2023, Mr. Baig received a phone call from REDACTED Chief Information Security Officer , REDACTED who informed him that a REDACTED employee fell victim to an impersonation scam on WhatsApp where an attacker posing himself as REDACTED scammed the REDACTED employee into giving the attacker about $20,000. Mr. Baig raised concerns about rising impersonations on WhatsApp with Mr. Tsimelzon and multiple other leaders in WhatsApp. Mr. Tsimelzon blamed the REDACTED employee for being stupid and refused to take any action. Mr. Tsimelzon continued to prioritize optimizing for his PSC by manipulating user harm metrics and Meta leadership allowed this to continue.

130. Mr. Baig received numerous reach outs from multiple other companies including World Bank about serious impersonation attacks which included impersonation of REDACTED CEO of World Bank and many others. Impersonations are a significant problem across all Meta Family of Apps and Meta refuses to take action as this impacts their user growth metrics.

Despite the ongoing retaliation, Mr. Baig continued to press for WhatsApp to address the systemic cybersecurity failures he identified throughout 2023.

131. In the first half of 2023, Mr. Baig repeatedly raised WhatsApp's cybersecurity vulnerabilities and did all that was within his power to fix the problems but was stymied by Mr. Verma's refusal to take action.

132. While Mr. Verma initially created a skeleton document in which he raised the possibility of Meta providing WhatsApp's security coverage, Mr. Verma has failed to

successfully collaborate with Meta's Central Security team to define the division of responsibility for user data security between Meta and WhatsApp.

133. Because Mr. Cathcart directed Mr. Verma to handle the issue, and Mr. Baig lacked the number of people reporting into him to address systematic issues of this size, Mr. Baig was not unilaterally able to begin to address the issues he raised, despite his best efforts to convince his management of the seriousness of the problem.

134. Even in the face of direct threats to his job, Mr. Baig continued to raise and press for the resolution of WhatsApp's serious cybersecurity deficiencies.

135. On March 15, 2023, Mr. Baig had a meeting with Meta's Central Security team, which can offer tooling and consulting support to WhatsApp. During that meeting, and in a subsequent recap he sent out, Mr. Baig reiterated that WhatsApp does not have a comprehensive list of all user data it collects, does not have a comprehensive inventory of all systems where WhatsApp stores user data, does not have a monitoring system in place for user data access, allows 1,500 WhatsApp and Meta engineers to have bulk access to user data in production, and cannot detect a data breach.

136. On the basis of these cybersecurity gaps, Mr. Baig flagged that WhatsApp is, or might be, in breach of the 2020 Privacy Order, in violation of SEC regulations and laws, and "risk additional legal action by the FTC, SEC, IDPC, and other regulators for not meeting our legal obligations." Mr. Baig alerted the Central Security team, "[w]e have not seen much or any progress on the state of security for WhatsApp."

137. On March 24, 2023, in response to Mr. Baig's disclosures during the meeting with Central Security, Mr. Verma spoke with Mr. Baig multiple times. On the first call, Mr. Verma took an angry tone with Mr. Baig. First, he told Mr. Baig that Mr. Baig was confusing the

Central Security team with his discussion of cybersecurity vulnerabilities and that the issues that Mr. Baig was raising were not important. Instead, Mr. Verma thought a more theoretical discussion on incident types for application security was more important, even though those issues did not relate to cybersecurity of user data, which was the primary issue.

138. Mr. Verma also claimed that by raising concerns about Meta's legal obligations, Mr. Baig was "making it about people and not about the issues," while in fact Mr. Baig's focus was on getting clear answers to the division of responsibility for user data security between Meta and WhatsApp from Meta's Central Security team.

139. Second, Mr. Verma told Mr. Baig that he did not want Mr. Baig to state that WhatsApp was non-compliant with the FTC order in writing. Mr. Verma told Mr. Baig that Mr. Baig was not a lawyer and should not be making those judgments, even though Mr. Baig knew the cybersecurity vulnerabilities and WhatsApp's obligations under the 2020 Privacy Order well. Mr. Verma added that if Mr. Baig had a concern, he should speak with a lawyer and make sure any statements about non-compliance with the FTC order were covered by the attorney-client privilege. Mr. Verma expressed concern that if there were a lawsuit, Mr. Baig's statements about WhatsApp's non-compliance with the FTC order could become discoverable. Mr. Verma directed Mr. Baig to speak with an attorney, Yannick Carapito, about his concerns.

140. In a brief second call, which occurred just minutes later, Mr. Verma attempted to dial back some of his earlier statements. He assured Mr. Baig that his earlier conversation was not a big issue but then pivoted and instructed Mr. Baig to only speak to a lawyer about Meta not meeting its legal obligations.

141. On April 14, 2023, Mr. Mukerji also expressed his anger at Mr. Baig for talking about FTC compliance, telling Mr. Baig, "I don't want you to talk about FTC [Privacy Order]

unless it is with [WhatsApp attorney] Yannick [Carapito]. I am serious." Mr. Baig understood that WhatsApp and Meta leadership clearly understood that they are violating the 2020 Privacy Order and were trying to shield it through the misuse of attorney-client privilege.

142. On April 18, 2023, through counsel, Mr. Baig sent Meta a detailed letter asserting claims of retaliation under SOX and California state law. In this letter, Mr. Baig included that he raised the aforementioned concerns about violations of the 2020 Privacy Order and SEC rules and regulations, including misstatements in Meta's SEC filings and public comments about its cybersecurity practices and systems. Since then, and in addition to his other protected activity, Mr. Baig has continued to assert claims of retaliation – based both on the aforementioned conduct and conduct post-dating his April 18, 2023, letter – through counsel.

As Mr. Baig continued to raise concerns about unremediated cybersecurity deficiencies at WhatsApp, the retaliation against him continued to escalate.

143. Despite such open hostility from Mr. Mukerji, Mr. Verma, and senior leadership, Mr. Baig continued to raise concerns about cybersecurity and data privacy deficiencies and Meta's misleading statements about WhatsApp's cybersecurity in violation of federal securities laws and regulations.

144. Mr. Baig spoke with Chad Greene, Director of Security, Meta, throughout April and May 2023 about the need for Meta to prioritize protecting against external cyber-attacks, specifically by creating a security program as required by the 2020 Privacy Order. Mr. Baig observed that many of WhatsApp's systems could allow for an external third party to hijack employee accounts and exfiltrate the personal data of millions of users. Among the many cybersecurity deficiencies that created this risk was the lack of 24/7 monitoring – under the current controls, it could take over several days before an intruder is detected. WhatsApp's

inability to locate all systems that contain user data and excessive employee access to data were also serious problems which had yet to be addressed. Mr. Baig told Mr. Greene that WhatsApp's overemphasis on preventing insider abuse left glaring gaps in its ability to prevent, detect, and respond to external attacks.

145. On May 16, 2023, Mr. Verma moved to a different role within WhatsApp and was no longer in Mr. Baig's management chain. Mr. Mukerji began directly reporting to Mr. Gupta.

146. Mr. Baig also spoke with Gregory Heimbuecher, Security Engineer, about the need to prioritize protecting against external cyber-attacks, but Mr. Heimbuecher shared that he and his team, Internal Detection Response ("IDR") team, were instead focused on preventing insider abuse, that is, the unauthorized accessing of personal social media profiles by Meta or WhatsApp employees. In most such cases, the IDR team detects a Meta or a WhatsApp employee spying on their former romantic partner several days after the incident has occurred. While this approach is acceptable for addressing insider abuse, the response time needed to detect an external attack needs to be in seconds because once user data is exfiltrated from Meta's corporate boundary, it cannot be recovered.

147. The IDR team is part of the larger "X-Sec" team (formerly known as the "Central Security" team, which is a cross-functional centralized security team at Meta which works on security matters across various platforms and products.

148. In May 2023, Guy Rosen, Chief Information Security Officer, Meta, announced that he has hired Bhavesh Mehta as Vice President of Engineering to lead all of X-Sec. Mr. Rosen in the announcement acknowledged that Mr. Mehta didn't have prior experience in cybersecurity. This surprised Mr. Baig, and he questioned why Meta, a multinational company

with extensive recruiting resources, would hire someone without any prior cybersecurity experience to lead X-Sec. The predecessor to Mr. Mehta, Clyde Rodriguez had a similar profile and had struggled to define the charter for X-Sec. Mr. Rodriguez had created a document titled "REDACTED" and invited everyone to help him define it.

149. Mr. Baig realized that Mr. Rosen and Michel Protti, Chief Privacy Officer, Meta, both have no prior cybersecurity and privacy experience:

a. Cybersecurity requirements and the 2020 Mandated Privacy Program have overlaps. Cybersecurity is typically defined as confidentiality, Integrity and availability of information, whereas the 2020 Privacy Order mandates controls for privacy, confidentiality and Integrity of information.

b. Mr. Baig understood that this lack of prior experience might be a contributing factor in the appalling state of cybersecurity and privacy at Meta which exposes Meta and its shareholders to serious legal risks.

c. Given the lack of experience, the terminology used in Meta for describing cybersecurity and privacy issues was very different from the rest of the industry e.g.: Meta used External Data Misuse ("EDM") to describe API Security, and SIR and ACPI to describe the likes of data discovery tools such as Amazon Macie, Spirion, etc.

d. Mr. Baig felt that the language used by the privacy and cybersecurity teams at Meta was like that of a language of a remote tribe in the Amazon jungle.

e. Mr. Baig also learnt that Mr. Rosen and Mr. Protti almost never raise cybersecurity and privacy risks to Mr. Zuckerberg for risk acceptance. There was no record of risks that were raised, remediated and / or accepted.

f. Mr. Rosen's team mostly focused on covering up illegal and unethical activities in Meta from leaking externally as opposed to protecting users and their data.

150. In early June 2023, Mr. Baig requested performance feedback from the X-Sec team. He had been working with them for several months and wanted to know if there were any ways to improve his collaboration with the X-Sec team.

151. In response to this feedback request, Mr. Heimbuecher submitted very positive feedback, applauding Mr. Baig for helping X-Sec prioritize tasks as they relate to WhatsApp and stating, "It's been a pleasure working with Attaullah in H1 across a broad variety of WhatsApp security initiatives." This feedback was reminiscent of the feedback Mr. Baig used to receive from Mr. Verma and Mr. Mukerji before he began raising concerns about cybersecurity failures.

152. In the summer of 2023, Mr. Baig traveled to London and defined the product requirements for a data discovery tool later renamed as the REDACTED REDACTED The product requirements were to be implemented by the team supervised by Nick Gardner, Software Engineering Manager, due to lack of staffing in Mr. Baig's team. Mr. Gardner's team was responsible for WhatsApp Privacy Engineering and Mr. Gardner was a peer to Mr. Baig who also reported into Mr. Mukerji at that time.

153. Later in June 2023, the IDR team released a report on the major cybersecurity threats facing WhatsApp and the roadmap for developing systems to remediate these cybersecurity gaps. This June 2023 IDR report, however, focused almost entirely on the risks

posed by insider abuse and made no mention of external threats or what actions WhatsApp should take to remediate the risk of external data exfiltration.

154. Mr. Baig sought to include his concerns about the threat of largescale data exfiltration in a pre-read document for a July 17, 2023, IDR/X-Sec check-in meeting which Mr. Gupta and Mr. Rosen were scheduled to attend. The IDR/X-Sec team refused to allow Mr. Baig to edit the pre-read document, so he added comments asking whether X-Sec intended to prioritize insider abuse over external threats and asking for a timeline to remediate these gaps.

155. After this meeting, the attendees, seemingly following the same playbook as Mr. Verma and Mr. Mukerji, attempted to paint Mr. Baig's reasonable concerns about cybersecurity deficiencies as an inability to collaborate with colleagues.

156. Mr. Heimbuecher met with Mr. Baig on July 18, 2023, to speak about the comments he left on the pre-read document. Mr. Heimbuecher was clearly upset about the comments Mr. Baig left in the pre-read document. He warned Mr. Baig, "Don't be the guy that people hate to work with," and stated that Mr. Baig's comments made the IDR team look like "idiots."

157. His colleagues also continued to exclude Mr. Baig's input from the pre-read documents that shape the discussions at critical meetings. For instance, Mr. Baig asked Mr. Heimbuecher and Ravinder Thind, Software Engineering Manager, if he could add notes to the pre-read for the August 30, 2023, check-in meeting with Mr. Gupta and Mr. Rosen to raise concerns about the decision to not prioritize WhatsApp's defenses against large scale external attacks. Mr. Heimbuecher and Mr. Thind forbade Mr. Baig from working on the pre-read document, tabling the matter for a later meeting.

158. During the summer of 2023, Meta opened an internal investigation into the claims of retaliation Mr. Baig raised in his April 18, 2023, letter. During these interviews, Mr. Baig cooperated by answering the investigator's questions about why he believed that WhatsApp's and Meta's failure to address these and other cybersecurity gaps would violate the 2020 Privacy Order and SEC rules and regulations.

159. WhatsApp has had a long-standing vulnerability in the "message reporting API" which allowed bad actors to submit false message reports against good users and get them banned from WhatsApp. WhatsApp was banning about 3 million users daily. In some cases, the bad actors were submitting false reports with child sexual abuse material ("CSAM"). In this case, a single false report will ban the good user, and the good user was also reported to National Center for Missing & Exploited Children ("NCMEC").

160. In the summer of 2023, Mr. Baig's team built an innovative solution that allowed detection of these false message reports. Mr. Tsimelzon unanimously decided not to use this solution and to allow the user harm to continue. Mr. Tsimelzon once again chose his PSC over user safety and user harm and continued to show progress by manipulating user harm metrics.

161. Mr. Tsimelzon expanded his team and embarked on a journey to build message franking that would significantly dilute the privacy of WhatsApp messages. WhatsApp and Meta leadership chose to allow hundreds of thousands of innocent users to be banned, reported to NCMEC, etc.

162. On August 7, 2023, Mr. Mukerji rated Mr. Baig as "Significantly Above Expectation" which translates to a year-end rating of Greatly Exceeds Expectation. Mr. Mukerji acknowledged the work Mr. Baig and team did, but Mr. Baig believed that Mr. Mukerji only provided him with this higher rating because Mr. Mukerji knew that Mr. Baig had raised claims

of retaliation, and that Meta was investigating his claims. In this meeting Mr. Mukerji said that Mr. Baig will very likely be promoted this time in February 2024.

163. At the August 30, 2023, check-in meeting, Mr. Baig raised this concern about large scale data exfiltration directly, stating that preventing a WhatsApp employee from accessing a specific profile is a wholly different security risk than an external party gaining access to WhatsApp's systems and exfiltrating user records from its servers. Mr. Baig stated that failing to develop a system to detect and respond to external attacks would put Meta in violation of the 2020 Privacy Order.

164. Concerned that Mr. Heimbuecher had no intention of revisiting the matter of prioritization after this meeting, Mr. Baig messaged Mr. Rosen to raise this concern directly with him. Mr. Rosen advised Mr. Baig to discuss this concern at the upcoming model building workshop which took place on September 11, 2023.

165. After this point, Mr. Rosen distanced himself from all meetings related to WhatsApp Security in which Mr. Baig was present. Mr. Rosen also did not raise these risks with the AROC Committee in Meta's Board. Mr. Baig believed that Mr. Rosen clearly understood the data exfiltration risk as being greater than Cambridge Analytica and hence distanced himself away from it.

166. In anticipation of this meeting, Mr. Baig prepared a pre-read document which highlighted the need for WhatsApp to prioritize developing a security program that complied with the FTC Privacy Order. Mr. Baig noted that, even though WhatsApp lacked 24/7 monitoring capabilities, a SOC to coordinate responses to attacks, and other critical cybersecurity infrastructure and procedures, WhatsApp's leadership had not put in place any plan to close these gaps, leaving the Company greatly exposed to a potential data breach.

167. This pre-read was circulated to the meeting's attendees, including Mr. Heimbuecher, Mr. Thind, Josh Ryder, Senior Security Engineering Leadership, Meta, and others from X-Sec.

168. At the meeting, Mr. Baig led a discussion of the concerns he raised in his pre-read documents.

169. Mr. Heimbuecher and Mr. Ryder were openly hostile to Mr. Baig. Mr. Heimbuecher did not want to discuss the gaps Mr. Baig identified and instead focused on his own team's projects to detect insider abuse, seeming to ignore that Mr. Baig had simply requested that WhatsApp needed to work on both insider abuse and external threats. Mr. Ryder vehemently disputed Mr. Baig's assessment. When Mr. Baig asked Mr. Ryder "what keeps you up at night?" in an effort to learn what Mr. Ryder considered the top priority issue at WhatsApp and Meta, he forcefully responded, "You! You do not think Meta has a comprehensive cybersecurity program." Mr. Ryder's hostility sufficiently alarmed Mr. Baig that he did not press Mr. Ryder to create a timeline for addressing external threats.

170. After the meeting, Mr. Ryder asked Mr. Baig to share a write-up on proposed preventative security measures, but Mr. Ryder never followed up with an action plan on the materials Mr. Baig sent him.

171. In September 2023, Mr. Baig published his vision for protecting WhatsApp user data and complying with the 2020 Privacy Order. Among many other things, it included the following:

a. Identifying all systems that contain WhatsApp user data.

b. Implementing an immutable audit trail for all user data access.

c. Significantly reducing employee access to be only based on documented business need.

d. Detecting and responding to anomalous user data access in near real time.

172. Over the next few months, Mr. Baig met several times with other colleagues working on WhatsApp's and Meta's cybersecurity issues to source their input for how best to work to remediate known external vulnerabilities. Among those from whom Mr. Baig sought advice was Mr. Greene. Mr. Baig explained that he had now repeatedly experienced friction between teams whenever he raises concerns about external data exfiltration, and he asked Mr. Greene on what he could do about escalating these concerns without generating such backlash. Instead of providing constructive feedback on how to escalate concerns, Mr. Greene simply told Mr. Baig to stop raising concerns.

173. On October 13, 2023, Steve Clarke, Director of Security, X-Sec, reached out to Mr. Baig, and they met. Mr. Clarke acknowledged the cybersecurity gaps of data exfiltration, and he specifically said, "How would the FTC feel, if they knew that it is possible for someone to take a three-terabyte file containing user data and move it outside of Meta?". However, Mr. Clarke advised Mr. Baig not to bring up the data exfiltration risk in the meetings with Mr. Rosen and Mr. Gupta.

174. Mr. Baig's mentor Damon Houghland, Director of Engineering, WhatsApp, also advised Mr. Baig not to raise the data exfiltration risk as it makes senior leaders look bad in front of Mr. Rosen.

175. Mr. Baig reached out to Mr. Heimbuecher to schedule a conversation about them working together and finding a common ground. They initially scheduled a call for October 4, 2023, but Mr. Heimbuecher indefinitely postponed the meeting.

176. Instead, on October 18, 2023, Alan Thomas, ERBP, informed Mr. Baig that he had received anonymous feedback about him.

177. Mr. Thomas summarized the feedback for Mr. Baig. Mr. Thomas wrote that other teams felt like Mr. Baig did not believe they were competent in their roles, that Mr. Baig asks for work product with turnaround times of under 24 hours, and that Mr. Baig frequently pivots away from agreed-upon priorities.

178. Mr. Baig explained to Mr. Thomas that this feedback was incorrect and retaliatory. Mr. Baig never opined on the ability of his colleagues to complete tasks nor did he disagree with agreed-upon priorities such as insider abuse; rather, he simply sought over the last few months to ensure that WhatsApp had a plan to also address the threat of large-scale data exfiltration by external actors, something entirely missing from the IDR's reports and planning documents. Mr. Heimbuecher had previously raised in June 2023 as "constructive criticism" a single example where Mr. Baig asked for something on 24 hours' notice, but this had not come up again since. It was clear that the submitter of this feedback intended to dig up as much negative feedback about Mr. Baig as possible. Mr. Baig reminded Mr. Thomas that, just a few months earlier in June 2023, he received very positive feedback from Mr. Heimbuecher. Mr. Baig felt that this negative feedback could only be retaliation for the cybersecurity concerns he had been raising since July 2023.

179. Shortly after discussing this feedback with Mr. Thomas, Mr. Baig filed an internal complaint with Meta's human resources that Mr. Heimbuecher had retaliated against him by submitting this negative feedback in response to the concerns about largescale data exfiltration raised by Mr. Baig.

180. Given his recent interactions with the IDR team and the repetition of Mr. Heimbuecher's previous feedback, Mr. Baig suspected that Mr. Heimbuecher had submitted this feedback anonymously.

181. On October 25, 2023, Mr. Baig reached out to Syed Abidi, Internal Auditor, Meta, and requested an audit for largescale data exfiltration risk. Mr. Abidi told Mr. Baig the proliferation of access to user data and largescale data exfiltration risks are very well known to the top leadership at Meta.

182. During this time, Mr. Baig continued to try and remedy the gaps with Account Takeover ("ATO") of WhatsApp users. As mentioned earlier, this is a big gap, and it was estimated that about 100,000 WhatsApp users were "getting hacked" (the colloquial term for when someone's account is compromised) and locked out of their accounts daily:

a. WhatsApp and Meta never disclosed these numbers to users or regulators.

b. WhatsApp and Meta chose to not issue breach notifications as required under GDPR or under the 2020 Privacy Order.

183. On October 16, 2023, Mr. Baig organized a full day workshop and invited Mark Hatton, Software Engineering Manager, WhatsApp, and Parth Shah, Software Engineering Manager, WhatsApp, and their teams. The outcome from this workshop was that these three teams will collaborate and work on two projects:

a. One of these projects was later renamed as Account Defense 2.0, which would require login approvals from a user's existing device to mitigate the ATO risk when the old and new device are far apart in geo-IP distance.

b. Another project named Post Compromise Account Recovery ("PCR"), which would allow users' whose accounts have been compromised, to recover their accounts from their existing device with one or more simple clicks.

184. Several months passed by and neither Mr. Hatton nor Mr. Shah followed up to collaborate with Mr. Baig on these projects, despite several reminders from Mr. Baig. Mr. Baig later learnt that Mr. Shah and Mr. Hatton have a large number of engineers who are working on Band-Aid solutions also known as busy or fake work and if the above two projects were to be implemented, their teams would have no work.

185. On October 30, 2023, Mr. Baig and the X-Sec team had a third check-in meeting with Mr. Gupta. Mr. Gupta acknowledged that Meta needed to address the threat of largescale data exfiltration, but the attendees at the meeting declined to take any steps to work with Mr. Baig to address these issues.

186. On December 5, 2023, Mr. Baig met with Ben Beard. Product Manager, Privacy Infrastructure, WhatsApp, who he had recruited to be the product manager for REDACTED. Mr. Baig described his vision for REDACTED especially as it related to the 2020 Privacy Order. Mr. Beard responded by saying "I don't worry much about the FTC Order. We have lawyers for that."

After opposing an effort to cover up with cybersecurity gaps raised by Mr. Baig and receiving extremely negative feedback from Mr. Mukerji, Mr. Baig escalated his concerns to Mark Zuckerberg.

187. On November 27, 2023, Mr. Baig raised a concern about the poor state of account security and account recovery on WhatsApp over an instant messaging chat with Mr. Brouwer and others. Mr. Baig shared the plan from the October 16, 2023, workshop with Mr. Brouwer. Mr. Brouwer agreed with the plan and said, "we should work on these two projects." However,

the only thing Mr. Baig saw was inaction and retaliatory feedback from Mr. Brouwer, while Mr. Brouwer focused on projects that helped with PSC and user growth metrics for WhatsApp.

188. On December 8, 2023, Mr. Baig attended a pre-meeting for the Quarterly Security Review ("QSR") for Q4 2023. Other attendees included members of the X-Sec team such as Chris Rohlf, Security Engineer, Michael Whiteman, Security Partner, and Lucas Fisher, Security Partner.

189. At this meeting, the X-Sec team presented on a test run of internal abuse security measures they had implemented and circulated a security report they had drafted. Mr. Whiteman told Mr. Baig the X-Sec team had designed these new security measures in response to the concerns he had raised.

190. This was surprising to Mr. Baig because he never raised concerns about internal abuse security measures in and of themselves. Rather, Mr. Baig was concerned that Meta had only devoted resources to internal abuse while ignoring clear deficiencies in the cybersecurity program to protect against external threats of data exfiltration.

191. Mr. Whiteman and his team also wanted Mr. Baig to engage in another exercise for six months to strengthen internal abuse detections. Mr. Baig disagreed and suggested a joint escalation to resolve the misalignment. In addition, Mr. Baig raised a concern that the X-Sec team cannot evaluate their own solutions as this is against cybersecurity norms. Mr. Baig said that the Internal Audit team or the Governance Risk and Compliance ("GRC") team is the right team to evaluate the cybersecurity solutions provided by the X-Sec team. Otherwise, the X-Sec team would essentially be auditing itself.

192. On December 13, 2023, an instant messaging chat was created for the Q4, 2023 QSR meeting. In this chat Mr. Baig once again raised the concern about the deficiencies in the

cybersecurity program to protect against external threats of data exfiltration. Mr. Rosen, Mr. Gupta, Mr. Mehta, Mr. Greene, Mr. Clarke, and other members of the X-Sec and the WhatsApp teams were part of this chat. Mr. Baig's concern upset a number of people in this chat, primarily Mr. Mehta, Mr. Greene and Mr. Clarke.

193. On December 14, 2023, during the Q4, 2023 QSR meeting Mr. Gupta created another instant messaging chat and asked Mr. Baig as to why he was pushing for a focus on external threats and whether he thought the X-Sec team and other cybersecurity leaders are a "bunch of idiots." Mr. Baig replied that he did not think they were idiots but that he just wanted them to acknowledge that largescale data exfiltration by an external actor is a substantial risk. Mr. Baig specified that Meta is missing several key hallmarks of an effective cybersecurity program – a SOC, proper security incident and event management system ("SIEM"), access controls, etc. – which in turn severely impairs WhatsApp's cybersecurity posture.

194. Later, the same day, Mr. Baig was able to have a one-on-one conversation with Mr. Gupta where he reiterated his concerns about largescale data exfiltration and the legal risks associated with it. Mr. Gupta advised Mr. Baig not to raise legal risks as that is for lawyers.

195. Instead, on December 15, 2023, Mr. Mukerji informed Mr. Baig that, on December 14, 2023, multiple members of the X-Sec team – later in January 2024 identified as Mr. Clarke and Mr. Greene – approached Mr. Mukerji to provide negative unsolicited feedback about Mr. Baig.

196. In January 2024, Mr. Baig also learned that Mr. Mehta had sent an email on or around December 15, 2023, to Mr. Gupta and others about Mr. Baig and subsequently submitted very negative feedback on Mr. Baig after he raised the largescale data exfiltration concerns in the Q4, 2023 QSR instant messaging chat.

197. Mr. Mukerji stated that these members of the X-Sec team criticized Mr. Baig for being uncollaborative and not trusting the X-Sec team and accused him of calling Mr. Rosen "an idiot" on December 8, 2023. Mr. Baig tried to explain what had happened, but Mr. Mukerji refused to listen.

198. Also on December 15, 2023, Meta again interviewed Mr. Baig to investigate his claims of retaliation. This interview took place in response to the concerns Mr. Baig had raised about the feedback anonymously submitted by Mr. Heimbuecher in October 2023. As before, Mr. Baig cooperated with the investigator and answered the investigator's questions about why he felt Mr. Heimbuecher and other Meta employees were retaliating against him for raising concerns about large-scale data exfiltration.

199. On December 26, 2023, Mr. Baig received an email from Mr. Mukerji accusing him of failing to collaborate with members of other teams. Most notably, Mr. Mukerji falsely stated that Mr. Baig's alleged collaboration issues caused X-Sec to drop the focus on large scale data exfiltration from the QSR, the exact cybersecurity gap which X-Sec had declined to address for months despite Mr. Baig's repeated raising of this concern. Mr. Mukerji also stated that these alleged issues fell short of the performance expectations as it relates to "collaboration" at Mr. Baig's level.

200. This email greatly mischaracterized Mr. Baig's role in advocating for the remediation of serious cybersecurity gaps that left WhatsApp user data exposed to exfiltration.

201. Fearing further retaliation, Mr. Baig did not immediately respond to Mr. Mukerji's email.

202. On January 2, 2024, Mr. Baig sent a letter to Mark Zuckerberg, CEO of Meta, and Jennifer Newstead, General Counsel, raising concerns about violations of the 2020 Privacy

Order, the SEC rules and regulations, and about the escalating retaliation against him at Meta. Mr. Baig shared a detailed timeline of the concerns he raised, the meetings he attended, the responses he received from other leaders, and the retaliation he experienced. He informed Mr. Zuckerberg and Ms. Newstead that WhatsApp had failed to safeguard user data, that the X-Sec team had falsified security reports in an effort to cover up the decision to not remediate the risk of data exfiltration, and that such falsifications can lead to and have led to criminal penalties. He included several documents outlining the details of Meta's and WhatsApp's cybersecurity gaps, the various pre-read documents showing that no effort was made to remediate the risk of largescale data exfiltration, and the remediation proposals he had previously circulated.

203. Despite this email, which clearly showed noncompliance with the 2020 Privacy Order, Mr. Zuckerberg continued to certify compliance to the FTC. In addition, Mr. Zuckerberg did not inform the AROC Committee and / or Privacy & Product Compliance Committee in Meta's Board about these gaps.

After Mr. Baig's letter to Mr. Zuckerberg, Mr. Mukerji continued to retaliate against Mr. Baig.

204. In early January 2024, Mr. Mukerji asked Mr. Baig to accept the false feedback he sent in December 2023 and to develop a plan to correct these alleged shortcomings. Mr. Mukerji and Mr. Baig agreed that Mr. Baig would respond in February 2024.

205. Around this time in January 2024, as a result of Mr. Baig's email to Mr. Zuckerberg, Meta expanded its internal investigation into the concerns Mr. Baig raised about retaliation since October 2023.

206. As part of this investigation, Mr. Baig sat for several more interviews with a member of Meta's internal investigations team, including interviews held on January 29, 2024, February 5, 2024, and February 7, 2024.

207. During these interviews, Mr. Baig cooperated by answering the investigator's questions about why he believed that WhatsApp's and Meta's failure to address these and other cybersecurity gaps would violate the 2020 Privacy Order and SEC rules and regulations.

208. Mr. Baig shared with the investigator many of the same documents he shared with Mr. Zuckerberg and Ms. Newstead and drafted additional summaries of the retaliation he had been experiencing.

209. Mr. Baig included in his summaries that Mr. Mukerji had directed additional funding and staffing of about 23 engineers, that was allocated as a result of the letter Mr. Baig sent to Mr. Zuckerberg for cybersecurity projects away from Mr. Baig and his team, targeted the performance ratings of Mr. Baig's team in order to make Mr. Baig look like a bad manager, and made him redo work for no reason in order to blame Mr. Baig for delays. Mr. Baig also wrote that Mr. Mukerji had been deliberately impeding Mr. Baig's efforts to combat ATOs and to develop Profile Scraping Mitigations, both major initiatives to reduce harm to users and to prevent cybersecurity breaches. Mr. Baig felt as though Mr. Mukerji was setting him up for a termination.

210. On January 7, 2024, Mr. Brouwer submitted very negative peer feedback on Mr. Baig and acknowledged that Mr. Baig had great ideas to mitigate cybersecurity risks and reduce user harm, but his ideas made Mr. Brouwer's team feel like they do not know what they are doing.

211. On January 17, 2024, Mr. Baig reached out to Mr. Gupta about prioritizing remediations for the ATO risk. Mr. Gupta told Mr. Baig in writing that it is not a priority for the company.

212. On January 30, 2024, Mr. Gupta requested upward feedback from Mr. Baig on Mr. Mukerji. Mr. Baig provided both positive and constructive feedback. In the upward feedback, Mr. Baig also raised a very significant concern in which Meta's top leadership declared a "false commitment" to the IDPC in which they claimed that WhatsApp had implemented solid technical controls that prevent WhatsApp user data from being accessed by Meta and other affiliates. This commitment is referred to as the "Uber Commitment."

213. Mr. Baig cited that there are several tables in the WhatsApp data warehouse that still could be accessed by 20,000 – 65,000 employees but there are less than 3000 employees that have undergone the WhatsApp data handling training. Mr. Baig said that this directly violated the Uber Commitment and the Section VII of the 2020 Privacy Order.

214. From this moment onwards, Mr. Gupta stopped communicating with Mr. Baig in one-on-one instant messaging chats.

215. On January 31, 2024, Mr. Baig raised another cybersecurity concern directly with Mr. Cathcart about a new feature that WhatsApp was building named "WhatsApp Contacts," after being blocked from raising it in the pre-read document. The concern stated that the WhatsApp Contacts feature will make the ATO situation significantly worse because an attacker can also get the entire phone address book of the victim, which would allow the attacker to scam friends and family of the victim much more quickly. This concern upset a large number of people who were working on this feature including Mr. Gupta, Mr. Tsimelzon, Uzma Barlaskar, Director, Privacy Product, and many others:

a. Mr. Cathcart swiftly accepted the risk as the priority of the company was to increase WhatsApp user base and reduce the risk of Apple limiting WhatsApp's access to a user's phone address book.

b. The WhatsApp Contacts teams continued to work on a misleading narrative which touted the security of how WhatsApp Contacts are protected with hardware security on the WhatsApp server, despite knowing the fact that the weakest link is ATO by one time passcode ("OTP") theft.

216. On January 31, 2024, Mr. Baig met with Mr. Abidi and Ms. Chandra, regarding an audit request to audit access controls in the WhatsApp data warehouse. Ms. Chandra told Mr. Baig that Mr. Rosen and team will block the audit, and they will say they already know about the issues. This is in direct violation of "The Securities Act of 1933" as Meta made the following statement "Our internal audit function provides independent assessment and assurance on the overall operations of our cybersecurity and privacy programs and the supporting control frameworks." in Form 10-k released on January 29, 2025.

217. On February 6, 2024, Aparup Banerjee, Engineering Director, WhatsApp, told Mr. Baig that his performance rating is at risk and the people that Mr. Baig is having issues with are "a small fish" in the ocean, implying that Mr. Baig had been setup to fail by WhatsApp and Meta leadership. Mr. Baig reported this to the internal investigator. From this moment on, Mr. Baig's relationship with Mr. Banerjee completely changed. Mr. Banerjee had in the past on six occasions submitted very positive feedback about Mr. Baig in Meta's performance management tool.

Despite receiving another retaliatory performance review in February 2024, Mr. Baig continued to oppose efforts by other teams to stop WhatsApp from remediating cybersecurity risks.

218. Unexpectedly, Mr. Mukerji suddenly took familial leave beginning in early February 2024.

219. On or around February 14, 2024, Mr. Baig responded to Mr. Mukerji's feedback, acknowledging receipt and emphasizing his efforts to advance security priorities for WhatsApp.

220. Shortly thereafter, Mr. Baig received his performance rating for 2023. Mr. Mukerji rated him as "Consistently Meets Expectations," resulting in a much smaller bonus and a much smaller formulaic equity and no discretionary equity compensation for the second year in a row. Additionally, Mr. Mukerji again denied Mr. Baig a promotion and sought to cast Mr. Baig as being uncollaborative. Mr. Baig believed that, if it wasn't due to the ongoing retaliation, he should have been promoted to Director of Engineering (D1) at Meta as part of February 2024 PSC cycle with a "Redefines Expectation" rating, formulaic compensation increases and discretionary equity.

221. In early 2024, Mr. Gupta and Nick Sunseri, VP of Data Science, WhatsApp, made a joint post on an internal messaging dashboard asking teams in WhatsApp to limit the usage of data warehouse for new use cases. Mr. Baig learnt that this initiative was due to the fact that WhatsApp user data was replicated thousands of times in the data warehouse, amounting to hundreds of Peta bytes of storage. Mr. Baig proposed that WhatsApp should audit the tables in the data warehouse, delete unused tables including those that were created by former employees as they pose an unwarranted cybersecurity risk. This potentially made Mr. Gupta and Mr.

Sunseri look bad as they were taking a Band Aid approach and not looking at this problem holistically.

222. In the spring of 2024, Mr. Baig began working more on WhatsApp's anti-scrapping efforts, that is, preventing bad actors from using WhatsApp APIs to collect users' personal information. He also continued to work on preventing ATOs.

223. In March 2024, Meta received a letter from the National Association of Attorney Generals about the worsening ATO situation on Facebook and Instagram and they demanded immediate action. As per Mr. Baig, WhatsApp was not mentioned in this letter because WhatsApp was not used heavily in the United States.

224. On March 13, 2024, Mr. Baig forwarded this letter to Mr. Cathcart urging immediate action. Mr. Baig also urged Mr. Cathcart to reconsider projects that will allow WhatsApp users to log in to their WhatsApp account with Facebook & Instagram credentials.

225. On March 15, 2024, Mr. Baig met with Mr. Thomas and expressed his concern about Mr. Mukerji continuing to retaliate against him even while he is on Family Leave. Mr. Thomas said he cannot discuss the type of leave Mr. Mukerji is on and advised Mr. Baig to work with Mr. Mukerji on the days Mr. Mukerji is available.

226. On March 26, 2024, Mr. Baig met with Mr. Hatton, Mr. Tsimelzon and their teams who were working on detection and measurement systems to determine whether an account had been taken over. Mr. Baig talked about the workshop they had on October 16, 2023, and the inaction from Mr. Hatton, Mr. Shah and their teams since that workshop. Mr. Baig proposed that WhatsApp could get ahead on ATOs by implementing login approvals from existing device, when the old and the new device are far apart in geo-IP location, something almost all social media or messaging platforms utilize. Mr. Baig reasoned that it would be best

to prevent accounts from ever being taken over instead of trying to catch them after the fact, especially because, despite years of work, this problem has never been fixed. Mr. Hatton recognized that preventive account security controls such as login approvals from existing device would likely eliminate the need for as robust of a detection system, rejected Mr. Baig's proposal, and replied, "If the security team fixes this [ATOs], then what will we do?"

227. Mr. Hatton's reply made Mr. Baig realized that many of his colleagues were obstructing his efforts to remediate cybersecurity issues because they worked on Band-Aid solutions to these problems and would no longer have roles, if these problems were fixed. They had strong incentives to maintain the status quo and work on projects that would allow them to claim they made progress every performance cycle without actually advancing WhatsApp's and Meta's account security protections for users.

228. In early March 2024, Mr. Baig created and distributed a report on WhatsApp's anti-scrapping projects and made several recommendations for how WhatsApp can improve its cybersecurity to comply with the 2020 Privacy Order. In this report, Mr. Baig raised a concern about profile impersonation risk from scraped profile photos. In particular, Mr. Baig recommended limiting users from accessing other users' profiles unless the other user has them in their contacts, has messaged them before, or is in the same group chat with them. Mr. Baig mentioned that WhatsApp is currently leaking Covered Information on millions, if not billions, of users daily and WhatsApp is severely under reporting scraping Covered Incidents to the FTC and other regulators. Mr. Baig also cited the strong protections that iMessage and Signal offer against profile scraping compared to WhatsApp:

a. WhatsApp had in the past allowed scraping of "Last Seen" and "Online" user data elements which enabled businesses such as chatwatch.net to thrive. If a

WhatsApp user suspected that their spouse or romantic partner is cheating with someone, they can provide the two phone numbers to chatwatch.net and it will be able to tell whether the two people in question are talking to each other.

b. Mr. Baig took the initiative on his own with no support and funding and built a patent pending solution to solve the above problem in early 2022.

c. In early 2022, Mr. Baig and his team also proposed restricting access to users' profiles in a similar manner, but WhatsApp and Meta leadership did not act on it, as this will affect the WhatsApp user growth metrics.

d. WhatsApp and Meta chose to not notify users or regulators about this data breach despite it being required under GDPR, 2020 Privacy Order and other regulations.

229. At the meeting on March 28, 2024, Mr. Gupta was extremely hostile towards Mr. Baig and did not allow him to speak. Mr. Gupta specifically said "I will not let a security guy speak as we will have to shut down the network" meaning it will impact WhatsApp user growth metrics that Meta reports to investors. Upon noticing Mr. Gupta's hostility towards Mr. Baig, various attendees who previously supported Mr. Baig's efforts completed changed their opinion on scraping risk and scraping Covered Incidents in order to appease Mr. Gupta. Mr. Baig pushed for an outcome from this meeting and the action item from this meeting was to escalate the profile scraping risk to Mr. Cathcart but both Mr. Gupta and Ms. Barlaskar blocked this escalation from happening. Mr. Gupta also refused to provide any staffing support that would allow Mr. Baig to remediate the profile scraping risk.

230. Around this time in another meeting, Ms. Barlaskar shared that she wants her own WhatsApp experience to be the most private, but she doesn't want this for other users by default as it will impact the WhatsApp user growth metrics. This surprised Mr. Baig as Ms. Barlaskar

was the Product Privacy lead for WhatsApp. This reminded Mr. Baig of Senator Dick Durbin's question "Would you be comfortable sharing with us the name of the hotel you stayed in last night?" to Mr. Zuckerberg during the 2018 congressional hearings.

231. In addition, Mr. Gupta and Ms. Barlaskar blocked progress on all projects from Mr. Baig's team that required their approvals. Mr. Baig's team primarily worked on projects that were related to meeting the legal obligations under the 2020 Privacy Order and other regulations.

232. On the data exfiltration risk, Mr. Baig continued to raise concerns regarding the Uber Commitment. Mr. Gardner and Ibai Urruchua, Product Manager, X-Sec, and many others started growing extremely hostile towards Mr. Baig.

233. On March 7, 2024, Mr. Baig met with Mr. Abidi, Ms. Chandra, Alexander Gacheche, Senior Director, Internal Audit, and raised concerns about the Uber Commitment and the Section VII of the 2020 Privacy Order.

234. On March 11, 2024, Mr. Baig met with Michael Johnson, Head of GRC, and his team and raised concerns about the Uber Commitment and the Section VII of the 2020 Privacy Order.

235. Mr. Johnson and Mr. Gacheche promised Mr. Baig that they will follow up on his concerns. However, neither of them followed up till February 10, 2025. Mr. Johnson was the former CISO of Capital One during the 2019 data breach and he is very aware of the consequences of a data breach. Mr. Baig expected that Mr. Johnson would take this cyber threat seriously, but he did not.

236. Mr. Baig shared detailed examples with Mr. Abidi about the tables in the WhatsApp data warehouse that violated the Uber Commitment and Section VII of the 2020

Privacy Order, *e.g.*: The REDACTED table in the WhatsApp open namespace was accessible to 65,000+ employees.

237. During this time, Mr. Baig continued working with Mr. Gardner and team on projects related to WhatsApp's obligation to limit employee access to user records and to identify the location of all user records.

238. Mr. Baig attended at least five meetings about limiting access to user records.

239. At one such meeting, Mr. Baig expressed a concern that, even though approximately 30,000 – 65,000 Meta employees had access to user data, only about 3,000 had undergone the WhatsApp data handling training. Mr. Baig proposed that Meta should further restrict access to user records to limit the potential for employee account compromise leading to data exfiltration. Attendees, including Mr. Gardner, rejected these proposals and refused to escalate the matter to senior management. They specifically said, "Uber Commitment doesn't solve for the security problem," and "we don't see a disagreement that needs to be escalated."

240. Mr. Baig also objected to WhatsApp's determination that it had successfully located 98% of user records. Mr. Baig questioned whether it was possible to make this determination since, crucially, Meta could not possibly be able to quantify the volume of unknown and missing records.

241. In addition, Mr. Baig questioned the accuracy of data in the "REDACTED" tool that was built as part of the Uber Commitment effort. The REDACTED tool had two different views. In one view, it showed that WhatsApp user data is stored in about 30,000 tables and the other view showed that WhatsApp user data is stored in about 3.5 million tables.

242. In addition, the number of tables in these two views kept fluctuating wildly without a reasonable explanation. This inconsistency in the REDACTED tool was also independently

observed by an internal auditor named Jubby Quiton who was performing an internal audit in compliance with the European Electronic Communications Code ("EECC") requirements.

243. In May 2024, Meta's Central Security team concluded a red team exercise named REDACTED which for the first time focused on data exfiltration risk. Mr. Baig understood that this exercise was conducted due to his January 2, 2024, letter to Mr. Zuckerberg. The findings from this exercise are deliberately blocked from being printed or copied and marked as attorney-client privileged even though the audit was not conducted for the purpose of receiving advice from counsel and this designation was meant to shield this report from discovery:

a. The scale of abuse with respect to attorney-client privileged shocked Mr. Baig as he had never seen anything like this in his 20 plus year career.

b. Mr. Baig started hallucinating that one-day Meta may be renamed as "Meta the attorney-client privileged company" and its ticker symbol changed to METAA/C.

c. Mr. Baig understood that, if Mr. Zuckerberg wanted, he can hire one attorney per every non attorney employee at Meta and mark everything inside the company as attorney-client privileged and continue breaking laws and regulations with impunity.

244. On May 24, 2024, the findings from REDACTED were presented to Mr. Gupta. Mr. Gupta started off the meeting and said, "We have known about these issues for a long time, why are we presenting them now." He also specifically said "blissful ignorance was better than this." Mr. Baig responded that we have to remedy these findings because we are legally required under the 2020 Privacy Order. Majority of the findings from this red team exercise were not remediated till February 10, 2025.

245. Mr. Gupta and Mr. Mehta did not report the serious cybersecurity findings from this report to the AROC Committee and instead chose to share a false positive victory from this exercise with AROC.

246. In late May 2024, Mr. Urruchua and Armen Mnatsakanyan, Software Engineering Manager, WhatsApp, claimed they are accountable for data exfiltration risk for WhatsApp, and they do not need Mr. Baig to be involved in this work.

247. Given the inaction from GRC and Internal Audit, and the extreme hostility from Mr. Gardner, Mr. Urruchua, and others, Mr. Baig decided to stop his engagement on the data exfiltration risk and informed the legal team about his decision.

248. On June 4, 2024, Mr. Baig met with Max Held, Privacy Program Manager, responsible for Uber Commitment. Mr. Held told Mr. Baig that Mr. Baig's Uber Commitment concern had been escalated to Central Privacy leadership.

249. On or around June 12, 2024, Mr. Baig learnt from Mr. Abidi that Mr. Baig's Uber Commitment concern had been escalated to the EVP (Executive Vice President) of Internal Audit, Susan Li, who is also the Chief Financial Officer of Meta. Mr. Abidi said that this concern was also escalated by the Privacy Internal Audit team to the highest levels in Central Privacy (Komal Lahiri, Vice President, GRC and Michel Protti, Chief Privacy Officer, Meta).

250. Mr. Abidi also told Mr. Baig that he had been blocked by others from performing an audit on the WhatsApp data warehouse related to Mr. Baig's Uber Commitment concern. Mr. Abidi told Mr. Baig to reach out to him later in the year 2024 to see if Mr. Abidi can perform an audit at that time.

After months of not having a supervisor, Meta assigned Mr. Baig to a new manager, though this ultimately did not alter the pattern of escalating retaliation against him but exacerbated it.

251. In May 2024, because of Mr. Mukerji's long leave of absence, Mr. Baig began reporting to Mr. Tsimelzon. Mr. Baig understood this retaliation was orchestrated by Mr. Zuckerberg as there were several problems with this reporting structure:

a. Mr. Tsimelzon was based in London, U.K, and this managerial reporting arrangement was very uncommon at Meta.

b. Mr. Tsimelzon in the past had blocked many projects led by Mr. Baig e.g.: REDACTED REDACTED Device Verification, REDACTED REDACTED etc. Mr. Tsimelzon's approach as outlined earlier was to falsify user harm metrics to get good PSC ratings, promotions and higher compensation.

c. In addition, Mr. Tsimelzon had 11 total direct reports which was extremely unusual. The other Engineering Directors reporting to Mr. Gupta's had just 3 direct reports.

d. Mr. Baig understood that this arrangement would allow Meta to cover up retaliation as Mr. Tsimelzon can easily start giving negative performance feedback to his other direct reports in addition to Mr. Baig.

e. Mr. Baig later learnt that this is exactly what was in play as Mr. Tsimelzon elicited negative feedback on his other direct reports to cover up the retaliation towards Mr. Baig.

f. Mr. Baig also understood that this elaborate cover up can only be the result of collusion at the highest levels in the company including Mr. Zuckerberg.

252. On May 29, 2024, less than a month after Mr. Baig started reporting to Mr. Tsimelzon, he sent a letter accusing Mr. Baig of serious collaboration issues and told Mr. Baig that he is not meeting expectations of his role. There were no specifics about the challenges, projects, or people, and the feedback was not actionable:

a. At this time, Mr. Baig further understood that it is not just his managers, but the entire Meta leadership, including Mr. Zuckerberg that were retaliating against him for raising non-compliance with the Securities laws and the 2020 Privacy Order.

b. Mr. Zuckerberg chose to give the additional 23 engineers meant to secure WhatsApp to the very same people that were retaliating against Mr. Baig and blocking him from remediating these gaps.

c. Mr. Baig also understood that the company was using the corporate playbook under the pretext of "look we changed his managers, and he is still having issues" meaning the company chose to retaliate against Mr. Baig versus reducing user harm and meeting legal obligations. This made Mr. Baig very sad.

253. Mr. Baig proactively reached out to and sought feedback from Mr. Gardner.

254. Mr. Baig expected Mr. Gardner to share feedback informally and verbally with him, but instead Mr. Gardner submitted feedback through Meta's performance management tool.

255. On June 10, 2024, Mr. Gardner wrote negative feedback that Mr. Baig suffered from collaboration issues. It is important to note that Mr. Gardner had earlier in June 2023, submitted very positive feedback about Mr. Baig's collaboration.

256. This feedback greatly concerned Mr. Baig because he knew it would be factored into his performance review. Mr. Baig submitted a complaint of retaliation through Employee Relations and the investigator from Mr. Baig's earlier interviews.

257. On June 12, 2024, Mr. Baig met with Nilesh Agrawal, Senior Software Engineer, WhatsApp Mobile Application Development. Mr. Agrawal empathized with Mr. Baig and offered his help to remedy the cybersecurity gaps. Mr. Agrawal advised Mr. Baig to not fight with too many people and said, "this company doesn't do anything for security unless forced by the FTC."

258. On June 12, 2024, Mr. Baig also met with Mr. Shah who in unequivocal terms told Mr. Baig that he did not collaborate with Mr. Baig on the two projects from the October 16, 2023 workshop because he and his team have to do busy work or design Band-Aid solutions, in order to comply with Meta's performance management process, that is, in order to receive positive performance ratings. His specific words were "this company runs on PSC."

259. On July 2, 2024, Mr. Baig met with Mr. Hatton. In that meeting Mr. Hatton voluntarily acknowledged that the work his team is doing is not focused on protecting users but to optimize for Meta's performance management process, that is, again, to increase their performance ratings.

260. Meta's investigator interviewed Mr. Baig again on July 11, 2024, and Mr. Baig cooperated by answering the investigator's questions and providing him with supporting documentation of the concerns he raised to his colleagues and leadership in WhatsApp.

261. On or around July 17, 2024, Mr. Tsimelzon asked Mr. Baig to write down his concerns with respect to the data exfiltration risk. Mr. Baig shared a detailed document with Mr. Tsimelzon. Mr. Tsimelzon took no action to fix the issues and instead reprimanded Mr. Baig for bringing up legal requirements with respect to the 2020 Privacy Order and told Mr. Baig that legal requirements should only be brought up by lawyers.

262. Around this time, Mr. Quiton contacted Mr. Baig about the EECC audit of WhatsApp's cybersecurity. His audit would focus on the EECC requirements. Mr. Quiton expressed concern that Mr. Gardner and his team were hiding information from Mr. Quiton about WhatsApp's user data and cybersecurity. Mr. Baig provided Mr. Quiton with the information he requested.

263. Shortly after, Mr. Baig informed Mr. Tsimelzon that he would be cooperating with Mr. Quiton's audit and that he thought it would uncover useful information about WhatsApp's data privacy compliance.

264. This upset Mr. Tsimelzon. Mr. Tsimelzon opined that audits are an opportunity for "agreement and collaboration," suggesting that WhatsApp employees ought to collude amongst themselves to provide a unified narrative to auditors instead of truthfully answering their questions.

265. Mr. Tsimelzon began openly retaliating against Mr. Baig and started soliciting negative feedback about him.

266. Mr. Tsimelzon solicited negative peer feedback from Ms. Barlaskar and Mr. Shah in the performance management tool. Mr. Baig was not given visibility into the peer feedback that was submitted by Ms. Barlaskar and Mr. Shah. It is important to note that Ms. Barlaskar had submitted positive feedback on Mr. Baig earlier in 2022 and had invited Mr. Baig to jointly file a patent together, which they did. In the past, Mr. Shah also had many positive things to say about Mr. Baig.

267. On August 8, 2024, Mr. Tsimelzon gave Mr. Baig a "Below Expectations" rating for his 2024 Mid-Year Review. In this review, Mr. Tsimelzon reprimanded Mr. Baig for bringing up legal requirements with respect to the 2020 Privacy Order. Mr. Tsimelzon also

suddenly reduced the scope of Mr. Baig's team to only Application Security. Mr. Tsimelzon said he reduced the scope based on the instruction he received from Mr. Gupta.

268. This was the first time Mr. Baig received such a low rating, and Mr. Baig worried that Meta would use this low rating to terminate him.

269. While Mr. Tsimelzon's negative review of Mr. Baig acknowledged his successes in implementing new security measures at WhatsApp, this review was highly critical of Mr. Baig's "collaboration" with other teams. Mr. Tsimelzon claimed he received unsolicited feedback about Mr. Baig's collaboration from eight individuals.

270. Mr. Baig recognized that these were individuals, such as Ms. Barlaskar and her team, Mr. Gardner and his team, Mr. Shah and his team, and the X-Sec team, who, over the last several months, had obstructed Mr. Baig's good faith efforts to remediate clear cybersecurity deficiencies and violations of the 2020 Privacy Order.

271. It greatly surprised Mr. Baig that he received such a negative review. Mr. Tsimelzon had been his supervisor for approximately three months at this point and barely had any opportunity to observe Mr. Baig working with other teams.

272. In the performance conversation with Mr. Baig, Mr. Tsimelzon also mentioned that he had relied heavily upon Mr. Mukerji's previous feedback, including the December 26, 2023, letter, and asserted that the recent complaints confirmed that the previous complaints about Mr. Baig were correct.

273. Mr. Baig again reported to Employee Relations and Meta's investigator his concern that he received this mid-year rating in retaliation for the cybersecurity concerns he raised and his efforts to assist with an audit of WhatsApp's cybersecurity.

274. On August 30, 2024, Meta's investigator again interviewed Mr. Baig about his concerns of retaliation. Like before, Mr. Baig cooperated with the investigation and provided supporting documentation.

275. In the summer of 2024, Mr. Baig made a polite post on an internal messaging board suggesting that WhatsApp should consider limiting the default privacy settings for all users to only people that the user knows, and consider building a message request feature, similar to Signal. Meta's leadership rejected this proposal as it will impact the WhatsApp user growth metrics.

276. In early September 2024, Mr. Baig learnt that Meta significantly overhauled the Annual Required Training ("ART"), and they took several inputs from Mr. Baig's reports to the internal investigator. The new training included references to Section V and Section VII (E) (3) of the 2020 Privacy Order. It also included a clear industry standard definition for scraping. Mr. Baig felt happy about the impact he had on the training. However, he understood that this is just progress on paper and the underlying cybersecurity and privacy issues were largely unmitigated, while the retaliation towards him kept escalating and it also started affecting most of his team.

277. Throughout the fall of 2024, Mr. Baig continued to advocate for remediating cybersecurity deficiencies.

278. For instance, in or around September 4, 2024, Mr. Baig and one of his direct reports published internally a report on the cybersecurity risks posed by allowing WhatsApp users to log into WhatsApp using their Facebook credentials. The ongoing project to expand the use of Facebook credentials was known as REDACTED. This report noted that WhatsApp accounts are four times more likely to be compromised if the user used their Facebook

credentials to log in. As Mr. Baig had previously proposed, this report recommended implementing login approvals from an existing user device to prevent ATOs.

279. Other leaders did not want this report widely distributed, so they deliberately buried its announcement at the bottom of a long email.

280. Mr. Baig learnt from Kabir Merali, Product Manager, WhatsApp Integrity, that WhatsApp wants to grow the United States user base to [redacted] million daily active users as soon as possible and WhatsApp will spend about [redacted] million in marketing to achieve this goal. Mr. Merali told Mr. Baig that we must relax the account security controls for [redacted] and help WhatsApp achieve this goal. This surprised Mr. Baig as Mr. Merali's role was to protect users and not grow users at any cost. In addition, these numbers mislead investors as Meta doesn't have a strategy to monetize from these WhatsApp users.

281. Mr. Hatton and several members from Mr. Brouwer's team opposed login approvals because this solution would affect the growth metrics and success of [redacted] which will also impact their own performance.

282. Mr. Brouwer and the broader [redacted] team ignored the risk assessment from Mr. Baig's team and instead circulated among leadership an update claiming that [redacted] will increase account security.

283. When Mr. Baig and his team asked over an instant messaging group chat why they had not included his team's risk assessment, the broader [redacted] team replied that it would "make us look bad" and that they "needed to grow WhatsApp at any cost" in the U.S.

284. One of Mr. Tsimelzon's team members, Andrea Santambrogio, said that, if leadership received the risk assessment from Mr. Baig's team, leadership may not let them

launch REDACTED an express admission that the use of Facebook credentials to log into WhatsApp posed a legitimate cybersecurity risk.

285. On October 17, 2024, Mr. Hatton met with Mr. Baig's team member who drafted the report on REDACTED and pressured him to revise the risk assessment to reduce the stated risk of ATOs. Mr. Baig's team member resisted this pressure.

286. Unable to make inroads with Mr. Baig's team member, Mr. Hatton created an instant messaging group chat with Mr. Baig and Mr. Tsimelzon to accuse Mr. Baig of collaboration issues and overstepping into his territory. Mr. Baig explained that Mr. Hatton and his team had proposed an ineffective plan to counter ATOs. Instead of prospectively verifying the identity of users, Mr. Hatton wanted to randomly sample users and send SMS OTP codes to confirm their identity, if and only if his detection algorithm noted a spike in ATOs at the end of the previous day. Mr. Baig reasonably believed it was not acceptable to let accounts be taken over and detect them later when there was a solution which could prevent the ATOs from ever happening in the first place. Mr. Baig explained that the regulators would never accept Mr. Hatton's solution.

287. Mr. Tsimelzon, however, refused to allow Mr. Baig to become further involved in this matter. He told Mr. Baig he could not have Mr. Baig architect a solution because of his issues with collaboration. Instead, he assigned the architect role for this project to Mr. Santambrogio.

288. Mr. Baig reported his concerns about retaliation to Meta's internal investigator. The internal investigator interviewed Mr. Baig again on October 25, 2024. As before, Mr. Baig cooperated with the investigation and provided supporting documentation.

289. During this time, Mr. Baig learnt that two of his patent proposals for PCR and Covert Messaging were denied. This is the first time Mr. Baig's patent proposals were denied. This further affirmed Mr. Baig's belief that it was not just his managers but all of Meta that was retaliating against him.

290. During this time, Mr. Baig continued to remediate the profile scraping risk.

291. On September 30, 2024, Mr. Baig and his direct report published a finding that WhatsApp is leaking at least 400 million profile photos of users daily to scrapers. WhatsApp leadership refused to act on this finding, continued to block progress on profile scraping mitigations and refused to provide additional staffing to close this gap.

292. On September 30, 2024, Mr. Baig also met with Central Privacy leadership, Sandeep Hebbani, Director of Engineering, Central Privacy, Meta, and advised Mr. Hebbani about the legal obligations of reporting this scraping activity as a Covered Incident to the FTC and other regulators.

293. Mr. Hebbani took several days to get back to Mr. Baig and to open a SEV (S[REDACTED] to track this scraping incident. Mr. Hebbani, however, deliberately did not allow Mr. Baig's team to log the attacker's/scraper's phone number, essentially making it impossible to report the Covered Incident(s). Mr. Baig's understanding is that Mr. Hebbani was likely blocked by top leadership in Central Privacy and Meta from reporting this scraping activity as a Covered Incident.

294. On October 8, 2024, a different internal investigator reached out to Mr. Baig. Mr. Baig learnt that one of his direct reports Daniel Sommermann had falsely accused Mr. Baig of retaliating against him for taking parental leave. There were several facts that were quite suspicious about this investigation:

a. This is the first time Meta interviewed Mr. Baig without his counsel present.

b. The investigation was scheduled with a very short notice (2-3 hours) from the invitation to the interrogation.

c. The investigator appeared to be in a rush and appeared to have an agenda.

d. She was asking a lot of questions in a real hurry and appeared to want to interpret the answers the way she wanted.

e. The investigator was unusually empathetic to Mr. Sommerman's newborn daughter affecting his sleep after his return to work from the long paternity leave.

f. Mr. Baig later observed a striking dissimilarity on how Sarah Wynn-Williams, former Public Policy Director's maternity leave was handled compared to how Mr. Sommerman's case was handled.

g. Mr. Baig learnt that the same investigator had pressured Mr. Baig's other team members into falsely admitting that Mr. Baig discriminated against them because they had children.

h. Mr. Baig strongly believed that all internal investigations have an agenda to advance the illicit interests of the company while silencing lawful whistleblowing.

295. For context, in March 2024, Mr. Baig gave Mr. Sommermann a strong performance warning for not making progress on two important projects:

a. Covert Messaging, a security feature which protects at-risk WhatsApp users from surveillance and traffic analysis attacks.

b. Advanced Secure Mode, a feature that is equivalent to Apple's lock down mode.

c. Mr. Sommermann had not made any progress as he was more focused on who's idea it was and who will get the credit for the idea, as opposed to protecting at-risk users sooner and meeting the expectations of his role.

296. Mr. Baig provided truthful answers to this investigator's questions. Mr. Baig understood that this investigation had been ongoing for some time now, while the other investigation was likely either paused or on hold. This surprised Mr. Baig as to which investigation Meta was prioritizing and why.

297. On October 10, 2024, Mr. Baig was cleared of the false accusation:

a. However, Mr. Thomas chose to give a documented email warning to Mr. Baig and asked him to refrain from giving legal advice regarding protected leaves.

b. At one point, Mr. Thomas also asked Mr. Baig for his bar association number.

c. Mr. Baig explained to Mr. Thomas that in Meta's performance evaluations, it is a common practice to refer to leaves as protected vs unprotected and this terminology is quite common and well understood across Meta.

d. Mr. Baig also explained to Mr. Thomas that Alaynna Elliot, Director HR, WhatsApp, had advised Mr. Baig in writing that engineers in WhatsApp and Meta are expected to produce the same amount of output as though they were working for the full year despite taking Paid Time Off or Recharge leave, as these leaves are not considered as protected leaves for performance evaluations.

298. On October 15, 2024, Mr. Quiton completed his audit but excluded five findings including the one related to Mr. Baig's concern related to Uber Commitment and Section VII of the 2020 Privacy Order.

299. In the meantime, Mr. Baig and his team built an innovative solution named as Covert Messaging, to protect WhatsApp users from surveillance attacks where a third party such as an Internet Service Provider can observe WhatsApp internet traffic and infer "who is talking to who" over WhatsApp. They scheduled a review with Mr. Cathcart for November 14, 2024. Mr. Gupta abruptly canceled the review and said this work product does not meet his bar. Mr. Gupta did not explain the gaps between this work product and his bar. Mr. Cathcart allowed this retaliation to continue.

As it became clearer that WhatsApp's leadership would not address its serious cybersecurity failures and would instead continue to retaliate against him, Mr. Baig filed a Form TCR with the SEC and informed Mr. Zuckerberg he had done so.

300. As a follow up item, Mr. Baig tried to reach out to Mr. Abidi regarding the internal audit of WhatsApp data warehouse and Mr. Baig's Uber Commitment concern. Mr. Baig learnt that Mr. Abidi is no longer employed at Meta. This was a shock as Mr. Baig thought highly of Mr. Abidi's ability to perform internal audits. Mr. Baig had also shared very positive feedback on Mr. Abidi in June 2024.

301. Over the next few months, Mr. Tsimelzon continued to block Mr. Baig's efforts to bring legal and regulatory risks to light and drive cybersecurity remediations.

302. For instance, on November 4, 2024, Mr. Baig wrote to Mr. Tsimelzon and others about WhatsApp's legal reporting obligations for scraping Covered Incidents. Mr. Tsimelzon told Mr. Baig not to bring up any legal obligations. This was the third time that Mr. Tsimelzon reprimanded Mr. Baig from raising legal risks. This was very similar to how Mr. Mukerji and Mr. Verma reacted when Mr. Baig began raising concerns about Meta's legal obligations to them.

303. Mr. Tsimelzon and team continued to harass Mr. Baig and team regarding ATO remediations and anti-scraping remediations because these remediations will make Mr. Tsimelzon and his team look bad and affect their PSC and employment prospects in Meta.

304. In late November 2024, Mr. Baig's team started worrying about their jobs and felt they will all be laid off as projects from the WhatsApp Security roadmap did not make it to the WhatsApp 2025 roadmap and the harassment continued.

305. On November 27, 2024, Mr. Baig's team member published a report in an internal message board on how ineffective the previous efforts from Mr. Tsimelzon and his team had been in reducing the scraping risk. Mr. Tsimelzon and team had been using rate limiting and account banning as techniques to combat scraping, but the scrapers were simply able to get new phone numbers for a few pennies, allowing them to bypass these bans. Mr. Tsimelzon and team were also unaware that WhatsApp has APIs which allow a scraper to retrieve 128,000 profile photos in one single API call.

306. This report upset Mr. Tsimelzon and he ordered Mr. Baig to immediately delete the report and reprimanded Mr. Baig and his team member for publishing such a report because Mr. Tsimelzon's supervisors and central leadership would see Mr. Baig's report, implying that this report would make Mr. Tsimelzon and his team look bad to leadership.

307. On November 27, 2024, Mr. Baig filed a Form TCR with the SEC about Meta's cybersecurity deficiencies and its failure to inform investors about these deficiencies. Mr. Baig wrote that Meta failed to track and manage its collection of user data and to identify where user data is stored. Mr. Baig explained that he had been experiencing retaliation since he raised this and other cybersecurity concerns, including failures to address scraping and ATOs. Mr. Baig

told the SEC that the highest levels of WhatsApp's and Meta's leadership were aware of these cybersecurity failures and yet have not taken the necessary steps to correct them.

308. Mr. Baig's team reported the retaliation and harassment to Mr. Thomas. Mr. Baig also reported the same to the investigator that he had been working with. In one such report, Mr. Baig described the new retaliation as "retaliation with impunity." In addition, some of Mr. Baig's team members used anonymous tools such as Pulse and Integrity line to report the retaliation and harassment.

309. Mr. Baig and his team, faced with continuous harassment, decided to give up ownership of profile scraping mitigations and the Account Defense 2.0 project to Mr. Tsimelzon's other direct reports.

310. On December 2, 2024, Mr. Tsimelzon's applauded Mr. Baig's decision and said Mr. Tsimelzon would have made this decision anyway. Mr. Tsimelzon also immediately asked about moving engineers from Mr. Baig's team to Mr. Hatton's team. In this meeting Mr. Tsimelzon also dismissed the internal audit timeline as a joke.

311. On December 4, 2024, Mr. Baig emailed Mr. Zuckerberg about the latest cybersecurity problems at WhatsApp and about the retaliation Mr. Baig continued to experience as he brought these issues to light since his last letter on January 2, 2024. Mr. Baig informed Mr. Zuckerberg that he had filed a complaint about Meta with the SEC.

312. On December 9, 2024, Mr. Baig met with Mr. Quiton in person. Mr. Quiton appeared scared and uncertain about his continued employment with Meta. Mr. Quiton completely changed his narrative about Mr. Gardner's lack of cooperation and said Mr. Gardner was providing correct answers to his questions in the summer of 2024.

313. On December 18, 2024, Mr. Quiton reached out to Mr. Baig and said he was under intense scrutiny and pressure, and he needed help to justify some of his audit findings and the associated risk levels.

314. Despite strong resistance and no support, Mr. Baig and team built PCR, an account recovery solution mentioned earlier in this complaint. Mr. Baig took this initiative on his own because he knew that about 100,000-400,000 WhatsApp users are locked out of their accounts daily due ATOs. Mr. Baig had also received numerous outreaches from WhatsApp users on LinkedIn who requested his help to allow them to their accounts faster, as scammers were targeting their family and friends from their accounts, while they are locked out.

315. In Mr. Baig's experience of working in other companies, a PCR type of solution would be implemented in 48 hours to 7 days. It took Mr. Baig several years of convincing, aligning, etc. to build this solution.

316. On or around December 16, 2024, Mr. Baig and his team finally launched PCR to 5% of WhatsApp users. Data showed that about 25000 users were recovering their accounts daily with PCR. Extrapolated, this meant about 500,000 users were being compromised daily and were getting locked out of their accounts, for at least the last 4 years.

317. On December 19, 2024, Mr. Tsimelzon colluded with Mr. Brouwer and team, created artificial collaboration issues, handed over the PCR project to Mr. Hatton and team, solicited negative feedback on Mr. Baig and his team, and ordered the PCR project to be rolled back and let the user harm continue. Mr. Baig again understood that the company was choosing retaliation over user safety, user harm and meeting legal obligations.

318. On January 8, 2025, Mr. Baig completed his self-review and clearly outlined non-compliance with the 2020 Privacy Order and the retaliation he has been facing due to raising

these concerns. In addition to sharing his self-review with Mr. Tsimelzon, he also shared it with the internal investigator that he had been working with.

319. On or around January 30, 2025, one of Mr. Baig's team members reached out to Mr. Cathcart and asked him to prioritize user safety over busy work, internal politics, etc. and further asked his help to unblock PCR. Mr. Cathcart refused to act despite several messages from Mr. Baig's team member.

320. In early 2025, a few weeks after his email to Mr. Zuckerberg, Mr. Baig observed several sudden changes in Meta. Mr. Zuckerberg appointed Joel Kaplan as the Chief Global Affairs officer, recruited Dana White to Meta's Board, eliminated fact checking in Meta's Apps, abolished DEI programs, removed tampons from men's bathrooms, settled a lawsuit with President Trump for $25 million and announced performance-based layoffs. In addition, Mr. Baig also learnt from a leaked press release that new SEC Investigations will need approval from the White House. It is unclear whether the changes to SEC Investigations were related to the above events or not. Mr. Baig is NOT alleging any wrongdoing on President Trump's part:

a. Mr. Baig understood that he will likely be targeted in this round of layoffs.

b. Mr. Zuckerberg said that the year 2025 will be an intense year and hence he is accelerating the performance-based layoffs.

c. This reminded Mr. Baig of the previous layoffs where Mr. Zuckerberg had said that the year 2023 is the year of efficiency. However, in Mr. Baig's experience, WhatsApp was and continues to be extremely inefficient as it has close to 3000 employees at a $[REDACTED] billion per year operating loss, and for the most part WhatsApp copies product features from Signal. Signal, on the other hand, has just 50 employees with an annual operating expense of $50 million.

d. Mr. Zuckerberg also routinely talked about the move fast culture at Meta. However, in Mr. Baig's experience, WhatsApp moves very slowly and has been working on a feature called "usernames" for the last 4 years which in no way can be considered as moving fast.

e. Mr. Baig understood that these are deliberate misleading statements to regulators, users, employees, investors, etc.

321. During his tenure, Mr. Baig also learnt that Meta invests heavily in internal and external communications with an intent to mislead the regulators, users, employees, investors, etc. Here are a few examples:

a. WhatsApp and Meta sued the NSO group, however they refused to implement basic protections for users such as PCR, Account Defense 2.0, Scraping Mitigations, Covert Messaging, Advanced Secure Mode, Data Security & Privacy protections, etc.

b. In January 2025, WhatsApp and Meta issued a public press release about Paragon Solutions attacking about 80 WhatsApp users. However, they have not issued a breach notification for about 500000 WhatsApp user accounts that are being compromised daily.

c. In March 2025, Meta issued a press release for firing leakers that leak internal posts, while user data can be directly exfiltrated from production servers without an audit trail.

d. Meta focuses on leakers who are exposing non-compliance, illegal and unethical behavior inside Meta.

322. On January 17, 2025, Mr. Baig filed a complaint with OSHA regarding the unlawful retaliation he has been experiencing and informed Meta about it.

323. In January 2025, Mr. Baig learnt that Mr. Gupta will be getting a budget to hire about 250 additional engineers and Mr. Baig's team will not get anything from this budget.

324. In January 2025, Mr. Baig also learnt from Alan Kao, Software Engineering Director, WhatsApp that only about 2-4 employees will be targeted for performance-based terminations in a typical organization of about 150 people.

325. Mr. Tsimelzon continued retaliating against Mr. Baig and his team during the year end performance evaluations:

a. He illegally retaliated against one of Mr. Baig's team members, denied him a promotion and reduced his rating from "Greatly Exceeds" to "Exceeds."

b. Mr. Baig reported the retaliation to Ms. Elliot and the internal investigator. However, nothing changed.

c. Mr. Baig understood that this type of retaliation is very common at Meta, as Meta forces mandatory arbitration for employment disputes which means most of these cases never go to trial, and in very rare cases when they do, the jury doesn't consider rating downgrades and promotion denials to be adverse enough actions.

326. In the performance calibrations, Mr. Baig also noticed a huge bias and falsehood as it relates to Mr. Zuckerberg's efficiency play:

a. Mr. Shah's team had grown from twenty to around sixty engineers in 2024, and one of their goals was to reduce SMS costs for WhatsApp.

b. This is the cost that WhatsApp pays mobile tele communication providers for delivering OTPs via SMS which allows new WhatsApp users to sign up for

WhatsApp and existing WhatsApp users to move their account from one device to another device.

c. WhatsApp's annual SMS spend is around $[REDACTED] million. This number has remained relatively flat over 2024.

d. Mr. Shah's team falsely claimed that they saved WhatsApp about $1.5 billion in SMS costs in 2024 and on this basis, one of Mr. Shah's team members was promoted from E5 to E6, while Mr. Tsimelzon, Mr. Gupta and Mr. Brouwer denied the well-deserved promotion to one of Mr. Baig's team member who built PCR, by citing "collaboration" issues.

327. On January 29, 2025, Mr. Hatton met with Mr. Baig and expressly admitted that the measured ATOs by his team are only a fraction of the actual ATOs, meaning Meta has been significantly under reporting ATOs, not taking appropriate action, and misleading users, investors, and regulators.

328. Shortly after the Q4, 2024 earnings call, Mr. Zuckerberg and Ms. Li said that Meta is meeting all its legal obligations. Mr. Baig wondered where Mr. Zuckerberg and Ms. Li are getting this information from and if they ever investigated Mr. Baig's concerns with respect to noncompliance with Meta's legal obligations:

a. This reminded Mr. Baig of the congressional hearings where Mr. Zuckerberg told the United States Congress that Meta has "industry leading tools to protect users."

b. In Mr. Baig's experience, this is not correct, as WhatsApp, Facebook, Instagram, etc. primarily focused on user growth metrics, ignored and blocked progress on ATO mitigations, scraping mitigations, impersonations, false message report mitigations, data security & privacy, etc.

329. On February 4, 2025, Mr. Baig participated in another internal investigation regarding his pretermination retaliation claims. Mr. Baig truthfully answered the questions.

330. On February 7, 2025, Mr. Baig told Courtney Cooper, Director Public Policy, WhatsApp, that WhatsApp will not meet the cybersecurity bar for it to be used by the U.S. House of Representatives. Mr. Baig shared a screenshot which showed that WhatsApp user data was accessible to 65,000 employees from across the globe and we cannot meet the on-soil requirements for WhatsApp use by the U.S. House of Representatives.

331. In Mr. Baig's experience, the HRBPs, the ERBPs, the internal investigators, the legal department, etc. all collude towards an outcome they have been ordered towards. Here are some examples:

a. Mr. Sommermann had no impact for making misleading harassment allegations while Ms. Wynn-Williams was publicly accused of toxic behavior and misleading harassment allegations.

b. Mr. Heimbuecher, Mr. Clarke, Mr. Greene, Mr. Mehta, Mr. Gupta, Mr. Tsimelzon, Mr. Gardner, etc. were not impacted despite aggressive retaliation and making false statements to regulators and auditors.

c. The investigator that Mr. Baig had been working with almost always steered towards the protected activity from 2022, despite Mr. Baig telling him that there are many more recent protected activities which made several other people look bad.

d. Mr. Baig felt that the internal investigations in Meta were like depositions from the opposing counsel.

332. On or about February 4, 2025, Mr. Baig reached out to Internal Audit and requested them to audit the ATO numbers that Mr. Tsimelzon and team have been manipulating to get good PSC ratings.

333. On February 7, 2025, Mr. Baig received strong positive upward feedback from his team and most of them acknowledged the significant adversity and retaliation they faced throughout 2024.

334. On February 10, 2025, Mr. Baig learnt that his employment with Meta is scheduled for termination due to "poor performance".

335. Mr. Baig understood that Mr. Tsimelzon, Mr. Gupta, Mr. Cathcart, Mr. Cox, and Mr. Zuckerberg had to go to extreme lengths to justify Mr. Baig's performance-based termination.

336. On March 3, 2025, Mr. Baig used the Meta's Integrity line and raised concerns with respect to noncompliance with the privacy regulations, Securities law violations, and requested the contact information of the AROC Committee and the Privacy and Product Compliance Committee in Meta's Board. Mr. Baig has not received a response.

337. Mr. Baig's believes, absent retaliation he would have received a "Redefines Expectation" rating at Director (D1) level and a promotion to Director (D2) level, in the February 2025 PSC cycle along with formulaic compensation increases and discretionary equity.

338. Mr. Baig has suffered extensive harm from Meta's retaliation against him. Because of his negative performance reviews, Mr. Baig has lost out on the opportunity for multiple promotions and has suffered substantial financial damage from the lower compensation he received in the last 2 to 3 years.

339. As a result of this treatment, Mr. Baig began to suffer physically and emotionally. Because of the stress of the retaliatory micromanaging, Mr. Baig suffered from anxiety, sleeplessness, restlessness, and health and family issues. Consequently, he gained weight, and his blood pressure shot up. This harm – financial, physical, and emotional has deeply impacted Mr. Baig and his family.

Unlawful Retaliation in Violation of SOX

(Violation of Section 806 of the Sarbanes-Oxley Act, 18 U.S.C. § 1514A)

340. Mr. Baig hereby incorporates by reference as though restated each of the factual allegations contained in paragraphs 1 through 339.

341. Under 18 U.S.C. § 1514A, it is unlawful for an employer to discharge, demote, suspend, threaten, harass, or in any other manner discriminate against an employee in the terms and conditions of employment for providing information which the employee reasonably believes constitutes mail, wire, bank, or securities fraud under federal law; a violation of any rule or regulation of the SEC; or a violation of any provision of federal law relating to fraud against shareholders to, inter alia, a person with supervisory authority over the employee (or such other person working for the employer who has the authority to investigate, discover, or terminate misconduct). *See* 18 U.S.C. § 1514A(a)(l).

342. Meta is a covered employer under SOX because it is a publicly traded company with equity securities that are registered with the SEC under the Securities Act. 18 U.S.C. § 1514A(a).

343. Mr. Mukerji, Mr. Tsimelzon, Mr. Gupta, Mr. Cathcart, Mr. Cox, and Mr. Zuckerberg are covered employers under SOX because they are employees of Meta and are responsible for the retaliatory decisions taken by Meta against Mr. Baig.

344. To establish a SOX retaliation claim, Mr. Baig must prove by a preponderance of the evidence that he "(1) engaged in a protected activity; (2) [t]he respondent knew or suspected that the employee engaged in the protected activity; (3) [t]he employee suffered an adverse action; and (4) [t]he circumstances were sufficient to raise the inference that the protected activity was a contributing factor in the adverse action." 29 C.F.R. § 1980.104(e)(2)(i)-(iv).

345. Under SOX, Mr. Baig need only show that his protected activity was a contributing factor in Meta's decision to take an adverse action against him. 18 U.S.C. § 1514A(b)(2)(C); 29 C.F.R. § 1980.104(e)(1).

346. Once a complainant has established that his protected activity contributed to the adverse action he experienced, a defendant seeking to avoid liability must show by "clear and convincing evidence" that it would have taken the same action even in the absence of the complainant's protected activity. 29 C.F.R. § 1980.104(e)(4).

347. Mr. Baig engaged in protected activity beginning in August 2022 when he warned WhatsApp leadership of WhatsApp's systemic cybersecurity failures. These instances included, but are not limited to: (1) Meeting with Mr. Cathcart and other WhatsApp leadership on August 18, 2022, and disclosing WhatsApp's cybersecurity failures; (2) drafting and sharing the pre-read, which flagged security issues, with Mr. Cathcart on September 8 and with Mr. Verma on September 26, 2022; (3) discussing cybersecurity failures detailed in the pre-read with Mr. Cathcart and Mr. Verma; (4) presenting his report at the meeting on October 18, 2022, with Mr. Cathcart and other WhatsApp Vice Presidents; (5) raising these issues in the Central Security meeting and subsequent post-read document he shared on March 15, 2023; (6) objecting to X-Sec's refusal to remediate the risk of data exfiltration throughout 2023, including to Mr. Rosen and Mr. Gupta; (7) requesting an internal audit of access controls in the data warehouse in

October 2023; (8) raising the risk of data exfiltration in Q4 2023 QSR conversations; (9) participating in internal investigation interviews throughout 2023 and 2024; (10) advocating to colleagues and leadership throughout 2024 the need to advance projects for anti-scraping, account takeovers, and controlling employee access to data; (11) reporting the "false commitment" to IDPC to Mr. Gupta, GRC, and Internal Audit in 2024; (12) raising cybersecurity risks with WhatsApp Contacts and [redacted] in 2024; (13) raising the cybersecurity risk of profile scraping and under-reporting of scraping Covered Incidents to FTC in 2024; (14) cooperating with internal cybersecurity audits in 2024; (15) filing a Form TCR with the SEC on November 27, 2024, detailing WhatsApp's and Meta's cybersecurity failures; (16) emailing Mr. Zuckerberg detailed letters on January 2, 2024, and on December 4, 2024, explaining cybersecurity deficiencies at WhatsApp and the retaliation he had been experiencing and informing Mr. Zuckerberg that he had filed a Form TCR with the SEC; (17) filing a pre-termination complaint with OSHA on January 17, 2025, and informing Meta about it; (18) raising concerns about illegal retaliation towards his team throughout 2024 and in the January 2025, performance evaluations; and (19) participating in the final internal investigation on February 4, 2025.

348. When he made these reports, Mr. Baig held a reasonable belief that he was objecting to wire fraud, securities fraud, violations of SEC rules and regulations, and shareholders fraud. *See Wiest v. Lynch*, 710 F.3d 121, 130 (3rd Cir. 2013) ("reasonable belief" requires that plaintiff have a subjective belief that the employer's conduct violates a provision under Section 1514A and that the belief be objectively reasonable); *see also Rocheleau v. Microsemi Corp., Inc.*, 680 F. App'x 533, 535 (9th Cir. 2017) (complaining employee's theory

of securities fraud is objectively reasonable if it approximates the basic elements of a securities fraud claim).

349. Moreover, publicly traded companies like Meta are prohibited from making false or misleading public statements about material facts. *See* 15 U.S.C. § 78j(b); 17 C.F.R. § 240.10b-5; 15 U.S.C. § 77q(a); *see* 17 C.F.R. § 240.10b-5(b) (making it unlawful "[t]o make any untrue statement of a material fact or to omit to state a material fact necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading"); *Matrixx Initiatives, Inc. v. Siracusano*, 563 U.S. 27, 46-47 (2011) (plaintiffs adequately pled federal securities laws violations where they alleged defendant made material misstatements about significant risks to its leading revenue-generating product).

350. When making these disclosures, Mr. Baig believed that Meta was violating SEC rules and regulations by failing to comply with the 2020 Privacy Order and because of the Company's public statements touting WhatsApp's security that could mislead a reasonable investor. Mr. Baig knew that Facebook had settled an FTC enforcement action against it for deficient data privacy for an unprecedented $5 billion, resulting in the 2020 Privacy Order. In tandem with that FTC settlement, Facebook had also reached a settlement of $100 million with the SEC for securities violations emanating from the same nucleus of facts as the FTC action against the Company. Additionally, Mr. Baig knew that Congress was encouraging the FTC to investigate Twitter for the exact same type of deficient cybersecurity posture that he was reporting, which further enforced his concern that Meta was in violation of its 2020 Privacy Order, which could subject it to more record-breaking fines and further action by the FTC and SEC.

351. Mr. Baig was particularly concerned about regulatory action because Meta had for years publicly touted WhatsApp as a safe and secure platform. For example, in August 2022, Product Head Ami Vora said, "We believe WhatsApp is the most secure place to have a private conversation,"[1] despite over 1,500 engineers having access to a user's data, including IP address, geographic location, contact information, and profile picture. Moreover, in the time since Mr. Baig raised his cybersecurity concerns with WhatsApp leadership, Meta has not changed its public statements about WhatsApp's security and has made misleading omissions in its public filings about the current state of its cybersecurity. On February 2, 2023, Meta released its 10-K for fiscal year 2022, in which it described WhatsApp as "a simple, reliable, and *secure* messaging application that is used by people and businesses around the world to communicate and transact in a private way."[2] (emphasis added.). On January 29, 2025, Meta released it 10-K for fiscal year 2024, in which it stated, "Our internal audit function provides independent assessment and assurance on the overall operations of our cybersecurity and privacy programs

[1] Liv McMahon, *WhatsApp: Mark Zuckerberg Reveals New Privacy Features*, BBC (Aug. 9, 2022), https://www.bbc.com/news/technology-62464243.

[2] Meta, Inc., 2022 Annual Report (Form 10-K) (Feb. 2, 2023), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/e574646c-c642-42d9-9229-3892b13aabfb.pdf. Moreover, Meta presented potential cybersecurity risks as mere hypotheticals. In its discussion of "Risks Related to Data, Security, and Intellectual Property," Meta stated, "Security breaches, improper access to or disclosure of our data or user data, other hacking and phishing attacks on our systems, or other cyber incidents *could* harm our reputation and adversely affect our business." (emphasis added). Meta stated further, "we have developed systems and processes that are designed to protect our data and user data, to prevent data loss, to disable undesirable accounts and activities on our platform, and to *prevent or detect security breaches*." (emphasis added). It added, "We experience such cyber-attacks and other security incidents of varying degrees from time to time" and "[w]e may also be unsuccessful in our efforts to enforce our policies or otherwise remediate any such incidents." As Mr. Baig had revealed, WhatsApp could not detect data breaches or guard against improper access to or disclosure of user data. Meta continued to make similar statements in its 10-K for fiscal year 2023. Meta, Inc., 2023 Annual Report (Form 10-K) (Feb. 2, 2024), https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/c7318154-f6ae-4866-89fa-f0c589f2ee3d.pdf.

and the supporting control frameworks". This is factually incorrect as many of the internal audits were blocked by Meta's top leadership in 2024.

352. Mr. Baig's belief that Meta was in violation of SEC rules and regulations was a good-faith, reasonable belief, under both a subjective and objective standard. *See Van Asdale v. Int'l Game Tech.*, 577 F.3d 989, 1000 (9th Cir. 2009) ("[T]o trigger the protections of the Act, an employee must also have (1) a subjective belief that the conduct being reported violated a listed law, and (2) this belief must be objectively reasonable.") Mr. Baig held a subjective belief that Meta was potentially violating SEC rules and regulations, as evidenced by his statements in the pre-read about the serious legal ramifications at the time. *See id.* at 1002 (SOX protections "include all good faith and reasonable reporting of fraud, and [that] there should be no presumption that reporting is otherwise, absent specific evidence" of bad faith"). Mr. Baig wrote, "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," referring to the SEC and FTC settlements. Mr. Baig also raised the possibility of financial penalties in the October 18, 2022, meeting. Moreover, after the October 18, 2022, meeting, Mr. Baig sent all the meeting invitees, including Mr. Cathcart, Mr. Gupta, and Mr. Verma, an article about Peiter "Mudge" Zatko, who had testified to Congress the month earlier that Twitter "leadership misled its Board of Directors, regulators, and the public" regarding its security failures and the FTC's ongoing investigation of Twitter for similar data issues. The Forbes article Mr. Baig sent stated that Mr. Zatko "accused the social media company of committing fraud and numerous 'egregious' security violations" and "claimed Twitter has made repeated 'false and misleading statements' to the FTC about its user security and privacy measures." The article emphasized the stock implications of Mr. Zatko's allegations, referring to the "Big Number" of "4.5%," which reflected "how much

Twitter stock is down in Tuesday morning trading amid a broader market rise." Additionally, in the March 15, 2023, Central Security meeting, Mr. Baig further indicated that WhatsApp is, or might be, in violation of SEC rules and regulations, the FTC privacy order, and other law.

353. Since then, Mr. Baig had frequently referred in conversations about cybersecurity failures to the 2020 Privacy Order and the potential for substantial fines and regulatory action. Of particular concern to Mr. Baig was the possibility that WhatsApp's and Meta's leadership could face criminal liability for misrepresenting the Respondent's cybersecurity capabilities and risks, similar to the charges brought against Uber's Chief Information Security Officer ("CISO") and the CISO of SolarWinds.[3]

354. Critically, an employee claiming protection under SOX's anti-retaliation provisions need not have used the word "fraud," nor cited a code section to have engaged in protected activity under the statute. *Id.* at 276. Rather, it is sufficient for purposes of alleging protected activity opposing securities, mail, and wire fraud that Mr. Baig complained about "knowing misrepresentation or knowing concealment of a material fact." *Dietz v. Cypress Semiconductor Corp.*, ARB No. 15-017, ALJ No. 2014-SOX-2, slip op. at 10–11 (Dep't of Labor Mar. 30, 2016) (emphasizing that employee's complaints about an illegal bonus scheme "included allegations of misrepresentations and/or concealment of materials facts," which "constitute[d] protected activity within the meaning of the SOX whistleblower provision").

355. Mr. Baig clearly suffered adverse action when WhatsApp and Meta downgraded his performance ratings, reduced his bonus compensation, and failed to promote him, all on

[3] SEC, "SEC Charges SolarWinds and Chief Information Security Officer with Fraud, Internal Control Failures," Press Release 2023-227 (Oct. 23, 2023), https://www.sec.gov/newsroom/press-releases/2023-227; DOJ, "Former Chief Security Officer Of Uber Sentenced To Three Years' Probation For Covering Up Data Breach Involving Millions Of Uber User Records," Press Release (May 5, 2023), https://www.justice.gov/usao-ndca/pr/former-chief-security-officer-uber-sentenced-three-years-probation-covering-data.

several occasions throughout 2023, 2024 and 2025. Mr. Baig received a "below expectations" rating in his 2024 mid-year review which risked dramatically reducing his compensation and may potentially even lead to termination if that rating is confirmed during the February 2025 performance cycle. Most recently, Mr. Baig received a notice of termination due to poor performance on February 10, 2025.

356. Similarly, the verbal warning – which included a documented, written recap that warned of "future discipline" – that Mr. Baig received on November 14, 2022, is an adverse employment action under SOX. *Fonseca v. Sysco Food Servs. Of Arizona, Inc.*, 374 F.3d 840, 847 (9th Cir. 2004) ("A warning letter or negative review also can be considered an adverse employment action" for a Title VII discrimination claim); *Mendez v. St. Alphonsus Reg'l Med. Ctr., Inc.*, No. 1:12-CV-00026-EJL, 2014 WL 6077608, at *22 (D. Idaho Nov. 13, 2014) ("[T]he Court finds that Miller's May 7 verbal warning and her May 18 written warning—both of which focused on the need for Mendez to improve his job performance, obey managers' instructions, and avoid negative or inappropriate communication with coworkers—constitute adverse employment actions" for purposes of Title VII discrimination claim.). The warning included a threat that "any future conduct along these lines could result in further discipline" and thereby satisfies the ARB's adverse action standard, which states that verbal reprimands are adverse employment actions when "coupled with a reference to potential discipline." *See Williams v. American Airlines Inc.*, ARB No. 09-018, ALJ No. 2007-AIR- 004, slip op. at 10-11 (ARB Dec. 29, 2010). Courts in the Ninth Circuit have favorably cited *Williams*. *See, e.g.*, *Guitron v. Wells Fargo Bank, N.A.*, No. C 10-3461 CW, 2012 WL 2708517, at *16 (N.D. Cal. July 6, 2012), *aff'd sub nom. Guitron v. Wells Fargo Bank, NA*, 619 F. App'x 590 (9th Cir. 2015). The subsequent warnings that coincided with his negative performance reviews are similarly adverse actions.

357. Mr. Baig's protected activity undoubtedly contributed to Meta's retaliatory actions against him. Since August 2022, retaliatory actions – whether they be verbal warnings, ostracization, negative reviews, or harassing feedback – have come right on the heels of Mr. Baig's protected activity. For instance, the "below expectations" mid-year rating given by Mr. Tsimelzon, based on Mr. Mukerji's earlier retaliatory feedback and performance reviews, came less than a month after Mr. Baig informed him that he had been cooperating with an internal audit into WhatsApp's cybersecurity deficiencies. *See Van Asdale*, 577 F.3d at 1003 (two and a half month gap between protected activity and termination could allow a reasonable fact finder to infer causation under SOX); *Coszalter v. City of Salem*, 320 F.3d 968, 977 (9th Cir. 2003) (In First Amendment retaliation case, "three to eight months is easily within a time range that can support an inference of retaliation."); *Yartzoff v. Thomas*, 809 F.2d 1371, 1376 (9th Cir.1987) (causation can be inferred when the first adverse employment action took place less than three months after an employee's protected activity); *Kelley v. Billings Clinic*, No. CV 12-74-BLG-SHE-CSO, 2014 WL 223377, at *19 (D. Mont. Jan. 21, 2014), *report and recommendation adopted*, No. CV 12-74-BLG-SHE, 2014 WL 496948 (D. Mont. Feb. 6, 2014) ("The Ninth Circuit generally has held that a period of less than three months between a plaintiff's protected activity and an adverse employment action is sufficient to raise an inference of causation."). Mr. Baig received a letter on February 10, 2025, informing him that his employment with Meta (formerly Facebook, Inc.) is being scheduled for termination due to poor performance as part of the February 2025 performance cycle. It came less than two months after Mr. Baig directly informed Mr. Zuckerberg that he had filed a Form TCR with the SEC and less than a month after he informed Meta that he has filed a SOX retaliation claim with OSHA.

358. Meta's, Mr. Mukerji's, Mr. Tsimelzon's, Mr. Gupta's, Mr. Cathcart's, Mr. Cox's and Mr. Zuckerberg's actions have caused and will continue to cause Mr. Baig substantial economic loss, including lost salary, bonuses, and equity; damage to his career prospects and earnings potential; damage to his professional reputations; humiliation; emotional distress; and pain and suffering.

359. By these actions, Meta, Mr. Mukerji, Mr. Tsimelzon, Mr. Gupta, Mr. Cathcart, Mr. Cox, and Mr. Zuckerberg have violated 18 U.S.C. § 1514A.

Requested Relief

Pursuant to 18 U.S.C. § 1514A(c), Mr. Baig asks OSHA to:

1. Investigate this complaint and issue a determination that Meta, Mr. Mukerji, Mr. Tsimelzon, Mr. Gupta, Mr. Cathcart, Mr. Cox, and Mr. Zuckerberg have violated 18 U.S.C. § 1514A;

2. Award Mr. Baig all appropriate damages to compensate him for Meta's, Mr. Mukerji's, Mr. Tsimelzon's, Mr. Gupta's, Mr. Cathcart's, Mr. Cox's, and Mr. Zuckerberg's retaliatory conduct;

3. Award Mr. Baig's attorneys' fees and costs that were reasonably incurred in connection with this complaint;

4. Award all other relief that the Secretary deems just and proper.