Renner K. Walker (Bar No. 295889)
rwalker@hausfeld.com
HAUSFELD LLP
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
Telephone: (646) 357-1100
Facsimile: (212) 202-4322

Attorney for Plaintiffs

(Additional counsel listed on signature page)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

VINEETH ANANTHULA, CALISTA SCHENCK, CRYSTAL CRENSHAW, THITIPUN SRINARMWONG, and DAVID BEVVINO-BERV, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

MERCOR.IO CORPORATION d/b/a MERCOR, DELVE AI, INC. d/b/a DELVE, BERRIE AI INCORPORATED d/b/a LITELLM, and DOE AI LAB DEFENDANTS 1 10,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Vineeth Ananthula, Calista Schenck, Crystal Crenshaw, Thitipun Srinarmwong, and David Bevvino-Berv ("Plaintiffs"), individually and on behalf of all others similarly situated, allege the following against Defendants Mercor.io Corporation d/b/a Mercor ("Mercor"), Delve AI, Inc. d/b/a Delve ("Delve"), Berrie AI Incorporated d/b/a LiteLLM ("Lite LLM"), and Doe AI Lab Defendants (collectively, where appropriate, "Defendants") based on personal knowledge as to themselves and their own acts, and on information and belief as to all other matters:

SUMMARY OF ACTION

1. On or about March 24, 2026, Mercor experienced a data security incident (the "Data Breach") in which a significant amount of personally identifiable information ("PII")[1] and protected health information ("PHI")[2] was exfiltrated by a group of hackers called "TeamPCP."[3]

2. The Data Breach exposed four terabytes ("TB") of data, including "[r]esumes, verified contact information, and Social Security numbers from people who applied through Mercor's platform," as well as "[h]igh-definition recordings of candidate interviews, passport and driver's license scans, and facial biometric data used for identity matching."[4] In short, the Data Breach has resulted in a staggering and devastating loss of PII and PHI.

[1] The Federal Trade Commission ("FTC") defines "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth . . . ." 17 C.F.R. § 248.201(b)(8).

[2] The Department of Health and Human Services ("HHS") defines "protected health information" as "individually identifiable" information created by a health-related entity that relates to an individual's health, healthcare, or payment for healthcare. 45 C.F.R. § 160.103.

[3] Jagmeet Singh, *Mercor says it was hit by cyberattack tied to compromise of open source LiteLLM project*, TECHCRUNCH (Mar. 31, 2026), https://techcrunch.com/2026/03/31/mercor-says-it-was-hit-by-cyberattack-tied-to-compromise-of-open-source-litellm-project/.

[4] *Mercor Breach Exposes 4TB of Data Including Biometrics and Source* Code, AI PRODUCTIVITY (Apr. 3, 2026), https://aiproductivity.ai/news/mercor-breach-4tb-data-biometrics-source-code/.

3. In a world of deepfakes and rampant phishing attacks, the loss of this detailed PII and videographic facial biometric data has opened Plaintiffs and the putative Class to extensive phishing attacks, identity theft, and violent in-person threats, harassment, and attacks. Indeed, Plaintiffs have already received multiple phishing attempts.

4. But this is not merely a data breach case. This case arises out of the use of an AI-driven labor platform that collected the functional equivalent of complete HR files on applicants and workers,[5] routed them through mandatory AI interviews, automated screenings, background checks, identity verifications, work trials, and ongoing surveillance, and then exposed that information through a foreseeable supply-chain compromise.

5. Mercor markets itself as a platform that matches talent to projects. In reality, it screens, scores, ranks, routes, evaluates, monitors, and effectively creates personnel files (and bottom-line scores) for people seeking or performing work for Mercor and its AI lab clients. It uses a number of tools, including Insightful: worker monitoring software that surveils workers including with video and screenshots to algorithmically draw conclusions about worker productivity.[6]

6. The Data Breach exposed far more than names and contact information. Mercor had assembled interview recordings, transcripts, identity-verification records, background-check data, profile images, resumes, work histories, tax and payment records, work product, project communications, monitoring screenshots, browser and app usage, client-facing work trials, and AI-generated or AI-assisted assessments—the practical equivalent of full HR files augmented with screenshots and videos of the worker.

[5] Mercor attempts to treat the workers it hires as independent contractors. That treatment is the subject of separate litigation. This Complaint refers to professionals that Mercor hires as "workers" throughout.

[6] *See* Insightful, *About Us*, https://www.insightful.io/about (last accessed April 20, 2026).

7. For workers subjected to Insightful or similar monitoring, that file was even broader: screenshots captured at frequent intervals, including as frequently as approximately every 30 to 60 seconds, could sweep in whatever was on a worker's personal computer screen. That could include medical portals, telehealth sessions, bank logins, legal research, personal photographs, family communications, romantic or sexual content, embarrassing websites, unrelated client files, or other material having no legitimate relationship to Mercor work.

8. Mercor and the Doe AI Lab Defendants then treated those records as evidence of a person's reliability, productivity, skill, judgment, and employability, without giving applicants or workers a meaningful way to see the full record, correct inaccurate entries, explain misleading screenshots, dispute algorithmic or client assessments, or segregate non-work material. Once leaked, those de facto HR files can follow workers for years through identity-theft markets, background investigations, professional reputation channels, social engineering, and future hiring decisions.

9. Mercor also used or caused the use of AI to analyze recorded interviews and interview-derived imagery, retained and reused interview results across applications, and automatically generated profile images from facial imagery supplied during interviews.

10. Mercor and the Doe AI Lab Defendants used this system to decide or materially influence who advanced, who was matched, who was offered work, who remained in the pipeline, and who remained staffed on projects. In some instances, final interviews were conducted by Mercor's client, and project continuity turned on a client AI lab's audit and approval.

11. This pipeline violated privacy, biometric, screening, consumer-reporting, and unfair business practices laws independent of the later Data Breach. The Data Breach magnified and crystallized those violations by exposing the very

data Mercor had amassed through opaque AI hiring, background screening, client-driven evaluation, and worker surveillance.

12. Federal regulators have warned that AI tools used to screen resumes and job applications, evaluate recorded video interviews, and monitor workers remain subject to federal employment-discrimination law, and that employers and users of third-party background dossiers or algorithmic scores for hiring or other work decisions must comply with the Fair Credit Reporting Act ("FCRA").[7] Yet, Mercor built and operated precisely the kind of black-box labor system regulators have warned about.

13. Moreover, Mercor's platform did not merely store ordinary user data. It collected and preserved the raw materials of identity, reputation, employability, and surveillance: faces, voices, interview demeanor, background dossiers, screening outputs, client-facing work trials, monitoring logs, screenshots, window titles, browser URLs, app usage, and private activity captured from workers' personal computers.

14. Upon information and belief, the Doe AI Lab Defendants were not passive end users. They participated in defining role criteria, interview formats, evaluation rubrics, source-material expectations, quality standards, audit decisions, continuation decisions, and hiring or staffing outcomes; received or used applicant and worker data produced through Mercor's platform; and in at least some instances directly interviewed candidates or determined whether projects would continue.

15. And, upon information and belief, Mercor sought to obtain third-party trade secrets, by pressuring workers to leverage preexisting materials and source files, which may have been confidential or restricted. Mercor's system encouraged or

[7] *See* Consumer Fin. Prot. Bureau, Circular 2024-06, *Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions* (Oct. 24, 2024); Fed. Trade Comm'n, *Using Consumer Reports: What Employers Need to Know*, https://www.ftc.gov/business-guidance/resources/using-consumer-reports-what-employers-need-know (last visited Apr. 21, 2026).

tolerated source-specific materials of questionable provenance; then its system (using Insightful) captured screenshots, metadata, work product, review notes, and client-facing assessments in a worker's de facto HR file without provenance controls, worker review, or correction rights. For some workers, this may have meant incentivizing or pressuring them to use their employers' confidential files; for others, it meant pressuring them to use patients' actual medical records. And Mercor did all of this without obtaining consent from workers' employers or other third parties like medical patients.

16. Meanwhile, Mercor built this system on a fast-moving AI infrastructure ecosystem that included LiteLLM and compliance assurances from Delve. When the LiteLLM supply-chain compromise occurred and resulted in the Data Breach, the outcome was foreseeable: a concentrated trove of applicants' and workers' full HR files, monitoring records, interview data, and source-adjacent work records was left exposed.

17. Delve's role was certifying that this ecosystem was safe and secure. But Delve, who promised that it could use AI and automation techniques to speed up certification and security compliance by significant scales—obtaining certifications in as little two months when the processes would normally take six to twelve months—has been revealed to have misrepresented whether its clients (like Mercor) were actually complying with industry standards for security.

18. Plaintiffs bring this action on behalf of themselves and a class of similarly situated applicants and workers seeking damages, statutory relief, restitution, declaratory relief, and structural injunctive relief requiring changes to Defendants' hiring, screening, monitoring, retention, correction, biometric, consumer-reporting, and data-governance practices.

PARTIES

19. Plaintiff Vineeth Ananthula is a natural person residing in Collin County, Texas. In February 2025, he created a Mercor account, submitted his credentials and

resume information, and completed a Mercor AI interview. He never accepted a Mercor position or performed services through Mercor. He later received a breach notice but never received proof that his AI interview, the underlying video, or the algorithmic analysis derived from it had been deleted or destroyed.

20. Ananthula provided Mercor with personal and professional information in reliance on Mercor's representations and now faces ongoing risks of misuse, impersonation, deepfake abuse, and continuing retention of his interview data and associated AI-generated assessments.

21. Plaintiff Calista Schenck is a natural person residing in Pasco County, Florida. She is in a federally protected age class and has a background in medical laboratory science, clinical microbiology, public health research, infectious disease epidemiology, laboratory information systems, medical records, antibiotic resistance, and clinical sales. She applied to approximately 20 healthcare opportunities through Mercor but never accepted a Mercor contract and received no Mercor earnings.

22. In connection with Mercor's application, AI interview, and work-trial process, Schenck provided banking information, government identification, Social Security number, interview and video data, and other sensitive personal information.

23. In one work trial, Mercor required Schenck to create a rubric, formulate an ideal response, and provide a patient-specific clinical-diagnostic image. She reasonably believed the assignment pressured applicants to use material that could be protected, confidential, or ethically unavailable. She refused to use real patient data, was not selected, and later discovered that Mercor had automatically opted her into a generative profile-photo feature derived from her interview imagery until she manually opted out.

24. After the Data Breach, Schenck experienced phishing and suspicious-account activity, including a purported Google account-takeover call and password-reset activity affecting payment applications. She changed passwords, strengthened security, and monitored her credit.

25. Plaintiff Crystal Crenshaw is a natural person residing in Cook County, Illinois. From approximately September 2025 through January 2026, she performed services through Mercor on projects that included generalist work, audio model training, digital annotation, and evaluation work. Despite her education and training in medical records, Mercor primarily matched her with generalized annotation and evaluation projects.

26. In connection with onboarding and participation on Mercor's platform, Crenshaw completed AI interviews and submitted a resume, LinkedIn information, KYC or identity-verification information, background-check information, and payment information. Mercor also created a generative profile image from her interview-related facial imagery. On information and belief, that required the capture, extraction, storage, or use of her facial geometry or other biometric identifiers or biometric information.

27. Crenshaw received a Data Breach notice and later experienced suspicious activity including an unauthorized attempt to access her Facebook account and spam calls. She also suffered an invasion of her biometric and privacy rights independent of the breach itself.

28. Plaintiff Thitipun Srinarmwong is a natural person residing in Queens County, New York. Beginning in or around July 2025, he completed multiple Mercor contracts in technical and coding domains, including Python and Java. During the breach period, his data, project history, communications, and work product were maintained in Mercor's systems.

29. In Mercor engagements, project managers and reviewers encouraged Srinarmwong and other workers to use real-life data or real experiences from their firms so long as the source was redacted or slightly changed. When he attempted to write at a higher level to protect confidential or sensitive information, Mercor reviewers criticized the work as too short and too vague and required rewrites. Mercor

did not provide meaningful mandatory training on how to avoid disclosure of protected, confidential, or regulated information.

30. Mercor maintained extensive applicant, interview, payment, project, and communications data concerning Thitipun, and his work through Mercor exposed him to ongoing professional, reputational, and confidentiality risks.

31. Plaintiff David Bevvino-Berv is a natural person residing in Palm Beach County, Florida. He holds a B.A. in Engineering Sciences from Yale University and an M.B.A. in Finance and Strategy from New York University's Stern School of Business. He has more than a decade of institutional-finance experience, including investment-banking roles at Credit Suisse and Goldman Sachs, co-founding a renewable-energy investment platform, and underwriting or closing more than $30 billion in clean-energy transactions.

32. In December 2025, Mercor recruited Bevvino-Berv for finance-expert work because of his financial modeling and clean energy expertise. Bevvino-Berv created a Mercor account, uploaded his resume, completed a work authorization process, signed onboarding documents, completed a paid financial-modeling work trial, and received an offer to join Mercor's finance team.

33. Bevvino-Berv then signed documents for two concurrent hourly remote engagements, including a Finance Expert role and a Step 1 Reviewer: Finance Expert role, each paying $150 per hour. His onboarding documents included Confidential Information and Inventions Assignment Agreements, Mercor Terms of Work, offer materials, a Form W-9 containing tax-identification information, and a Worker Agreement.

34. During onboarding, Bevvino-Berv provided Mercor with his full legal name, home address, email addresses, phone number, resume and work history, government-issued photo identification, Form W-9 tax-identification information, bank-account information connected through Stripe, and Excel-based financial-modeling work product. He was also required to complete a background check

through a third-party provider such as Certn or Zinc and completed recorded interactions as part of the screening process.

35. Bevvino-Berv worked on a finance-related project supporting a Doe AI Lab Defendant's development of large language models. His work involved creating and reviewing complex financial-modeling tasks, including operating models, LBO analyses, DCF valuations, and other institutional-grade financial exercises, using the client platform, Microsoft Excel, Google Docs, Slack, and a custom reviewer tool built on a major AI platform.

36. In January 2026, Bevvino-Berv was promoted to Step 1 Reviewer on that project. In that role, he reviewed other contributors' model submissions, performed model rebuilds from input templates, compared results against gold solutions, and identified errors.

37. Bevvino-Berv worked consistently from late December 2025 through early April 2026. Insightful time-tracking records reflected approximately 151 hours and 28 minutes of monitored time, including writing tasks, review tasks, and model-rebuild work.

38. As a condition of his engagement, Mercor required Bevvino-Berv to install Insightful, a time-tracking and productivity-monitoring application, on his personal computer. Mercor did not provide a separate work device, and Bevvino-Berv was not clearly informed that Insightful would track computer activity beyond his Mercor-related work.

39. In practice, Insightful tracked far more than Bevvino-Berv's Mercor work. Records exported from the platform show that, over the relevant monitoring period, Insightful captured usage across at least 240 distinct applications and websites, many unrelated to Mercor duties, including personal bank accounts, health-insurance portals, telehealth platforms, Google Photos, personal email, utility accounts, credit-card and loan accounts, and other private websites and applications.

40. Mercor also required Bevvino-Berv to use an account with a generative-AI platform as an integrated part of his workflow, including by providing a premium subscription tied to his personal account for automated quality checks on work product. Because this was his personal account and monitoring remained active during work sessions, personal non-work conversations—including conversations relating to private legal and medical matters—were exposed to Mercor's surveillance environment.

41. On March 31, 2026, Bevvino-Berv received Mercor's breach notice. The notice did not identify the nature of the attack, specify the categories of personal information compromised, describe protective steps, use the word breach, or offer credit monitoring, identity-theft protection, or any other remediation.

42. Shortly after the breach notice, Bevvino-Berv's contracts were placed on pause because the client AI lab was conducting an audit and Mercor was awaiting the audit's results before resuming work. Bevvino-Berv later received an invitation to a final-stage interview for a clean-energy transaction-professionals role developing AI-enabled workflows, and Mercor confirmed that the interview would be a conversation directly with the client.

43. Bevvino-Berv has suffered concrete harm, including loss of privacy, emotional distress, time spent mitigating risk, credit freezes, password changes, credit-monitoring enrollment, increased phishing and scam attempts, lost income from paused engagements, and career-related concern that monitoring data, review notes, client assessments, or misleading screenshots may be exposed or reused without his ability to inspect or correct them.

44. Defendant Mercor.io Corporation d/b/a Mercor is a Delaware corporation with its principal place of business in San Francisco County, California. Mercor operates an AI-driven recruiting, screening, and contractor-management platform.

45. Defendant Delve AI, Inc. d/b/a Delve is a Delaware corporation with its principal place of business in San Francisco County, California. Delve markets automated compliance and certification services, including security and privacy certifications.

46. Defendant Berrie AI Incorporated d/b/a LiteLLM is a Delaware corporation with its principal place of business in San Francisco County, California. LiteLLM develops and distributes an AI gateway or proxy tool used to connect software systems to large language models and related services.

47. Defendant Doe AI Lab Defendants 1 through 10 are corporations, limited liability companies, partnerships, or other business entities whose true names and capacities are presently unknown. Upon information and belief, these defendants used Mercor's platform and services to recruit, screen, score, rank, route, interview, monitor, evaluate, staff, or retain applicants and workers; obtained or caused Mercor to obtain applicant and worker data; received or used reports, scores, evaluations, background-screening outputs, interview records, or work-trial results; and participated in decisions regarding who advanced, who was hired or staffed, and who remained assigned to projects.

48. Plaintiffs will amend this Complaint to allege the true names and capacities of the Doe AI Lab Defendants when they are ascertained.

JURISDICTION AND VENUE

49. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs; the proposed class contains more than 100 members; and minimal diversity exists.

50. This Court has supplemental jurisdiction over Plaintiffs' related state-law claims under 28 U.S.C. § 1367.

51. This Court has personal jurisdiction over Mercor, Delve, and LiteLLM because each is headquartered in or directs substantial business from this District.

Upon information and belief, the Doe AI Lab Defendants purposefully availed themselves of this District by contracting with Mercor here, directing hiring, screening, auditing, project-management, or staffing decisions through Mercor here, and causing the collection, processing, use, and disclosure of applicants' and workers' data through Mercor's systems in this District.

52. Venue is proper in this District under 28 U.S.C. § 1391 because Mercor, Delve, and LiteLLM reside in this District and a substantial part of the events or omissions giving rise to these claims occurred in or were directed to this District.

53. Because Defendants reside in San Francisco County, and/or purposefully availed themselves of this District, a significant amount of the events giving rise to Plaintiffs' claims occurred in San Francisco County, pursuant to Local Civil Rule 3.2(d), assignment to the San Francisco Division is proper.

FACTUAL ALLEGATIONS

A. Mercor Built an AI-Driven Pipeline that Collected the Equivalent of Complete HR Files.

54. Mercor is not merely a job board. It is an AI-driven labor platform that collects, processes, stores, reuses, and monetizes applicant and worker data at virtually every stage of the relationship—from initial screening through ongoing work performance and post-engagement retention.

55. Mercor publicly states that it collects and processes, among other things, names, email addresses, phone numbers, resumes, work history, skills, qualifications, interview recordings, interview transcripts, responses to interview questions, profile photos and images from interviews, salary expectations, employment preferences, account credentials, device data, usage data, location data, cookies, and information from third parties.

56. Mercor's materials also indicate that it uses AI to analyze candidate interviews and may generate professional photos from interview images. To generate

professional photos, Mercor must necessarily capture biometric data like facial geometry.

57. Mercor's AI interview materials further indicate that if another application requires the same interview, the applicant's existing result may be retained and reused.

58. Accordingly, Mercor was not collecting a narrow or low-risk set of information. It was collecting the functional equivalent of full HR files: resumes, interview recordings and transcripts, identity verification records, background-check inputs, payment and tax data, work-trial submissions, client-specific evaluations, profile images, account credentials, and related communications.

59. Mercor's onboarding and work-trial processes often demanded the submission of highly sensitive information before any full engagement existed, including identity-verification data, bank details, tax information, confidentiality and IP assignments, and background-check information.

60. Applicants who never performed a single hour of work for Mercor—including Plaintiffs Ananthula and Schenck—were nevertheless required to surrender highly sensitive personal, professional, financial, interview, and in some instances biometric information.

61. Applicants like Plaintiffs Ananthula and Schenck were never presented with conspicuous notice that Mercor gathers biometric information and retains it indefinitely.

62. Indeed, Mercor does not publicly post that its platform routinely gathers and stores biometric information indefinitely.

63. Applicants are not required to form any kind of contractual agreement with Mercor as a condition of applying.

64. Workers who did perform services through Mercor—including Plaintiffs Crenshaw, Srinarmwong, and Bevvino-Berv—were required to provide the same core information plus additional project, performance, communications, and monitoring

data while Mercor and its client AI labs preserved the economic advantages of labeling many workers independent contractors even where screening, routing, monitoring, and client control resembled ordinary employment.

65. The concentration of this data was itself dangerous. It created a single system containing identity data, financial data, interview data, background-screening data, visual and audio data, work product, evaluations, monitoring records, source-adjacent materials, and client-facing assessments that could be misused for identity theft, impersonation, blacklisting, deepfakes, social engineering, professional harm, or coercion.

66. This collection of data made it foreseeable that a data breach would cause serious harm to Mercor's applicants and workers.

B. Mercor and the Doe AI Lab Defendants Used Mandatory AI Interviews, Automated Scoring, and Direct-Client Screening to Control Access to Work.

67. Mercor required applicants to move through recorded AI interviews, assessments, work trials, identity-verification steps, and, for many roles, background screening before they could access work opportunities.

68. These systems were not merely administrative conveniences. Upon information and belief, Mercor and the Doe AI Lab Defendants used them to decide or materially influence who advanced, who was matched to opportunities, who received offers, who remained in the pipeline, who was sent to a client interview, and who remained staffed on projects.

69. Mercor's applicant communications were themselves at least partially automated. When Schenck sought clarification about whether project work for the Medical Expert and Science Expert roles would resemble Mercor's rubric-heavy bootcamp exercise, Mercor responded through "Melvin," which identified itself as Mercor's AI Assistant. Melvin proved to be the primary entity that responded to

Schenck's inquiries. There was no indication that any human employee at Mercor was reviewing or supervising Melvin's communications.

70. The AI-interview and work-trial process also appears designed to standardize applicants into machine-readable rubrics and outputs. Schenck, an experienced medical professional in a protected age class, was routed through repeated standardized tasks and opaque rejections despite her domain expertise and numerous applications.

71. Mercor's own materials say AI can evaluate candidate interviews and that interview results may be reused across applications. Mercor never provided Ananthula proof that his interview video, interview-derived analytics, or algorithmic assessment had been deleted or destroyed.

72. Mercor's clients were not passive spectators. In one final-stage interview process, Mercor told Bevvino-Berv that he had been shortlisted for a role building AI-enabled workflows for clean-energy transaction professionals, that the interview would assess role fit and availability, and that the interview would be a conversation directly with the client.

73. The same pattern appears in one of Bevvino-Berv's assignments. Bevvino-Berv worked on an initiative supporting a Doe AI Lab Defendant's development of large language models, communicated with Mercor leads and other workers in client-specific channels, was promoted to reviewer, and after the breach saw his contracts paused because the client AI lab was conducting an audit and Mercor was waiting for the client's decision before resuming work.

74. Upon information and belief, the Doe AI Lab Defendants helped define role criteria, review work-trial outputs, conduct or require final-stage interviews, evaluate worker output, approve or reject contractors, receive screening and work-product reports, and determine whether workers were accepted, retained, paused, or removed.

75. Federal regulators have warned that AI and other automated tools used to screen job applicants, analyze recorded video interviews, and monitor workers remain subject to federal employment-discrimination law.[8]

76. The EEOC has also explained that Title VII applies to employers' use of automated systems to make or inform selection decisions and that such systems can create unlawful adverse impact on protected groups, including older workers, unless justified and properly validated.[9]

77. These protections extend to recruitment, hiring, referral, and employment-agency functions, even where decision-making is outsourced or mediated through software and other automated tools.

78. Yet, Mercor and the Doe AI Lab Defendants gave applicants and workers no meaningful transparency into how AI scoring worked, what characteristics were weighted, whether interview-derived analytics would be reused, whether background or identity reports would be shared with clients, whether human review would occur, or how applicants could challenge or correct adverse outputs.

79. Upon information and belief, that opacity was not accidental. It preserved the speed and economic advantages of an AI-mediated labor pipeline while denying applicants and workers the transparency, accountability, and legal protections that would ordinarily accompany comparable employment decisions.

C. Mercor Extracted and Used Biometric and Interview-Derived Data Without Required Notice, Consent, Transparency, or Deletion.

80. Mercor required applicants and workers to submit recorded video interviews capturing their faces, voices, expressions, and speech, and it stored images derived from those interviews.

---

[8] *See* Equal Employment Opportunity Commission, *Employment Discrimination and AI for Workers* (Apr. 29, 2024), https://www.eeoc.gov/sites/default/files/2024-04/20240429_Employment%20Discrimination%20and%20AI%20for%20Workers.pdf.

[9] *See* EEOC, *2023 Annual Performance Report* (Mar. 11, 2024), https://www.eeoc.gov/2023-annual-performance-report; EEOC, *Employment Tests and Selection Procedures* (Dec. 3, 2007), https://www.eeoc.gov/laws/guidance/employment-tests-and-selection-procedures.

81. Mercor also used or caused the use of interview imagery to generate or offer professional or generative profile photos. Schenck was automatically opted into that feature until she manually opted out. Mercor created a generative profile image for Crenshaw as well.

82. Upon information and belief, the analysis of recorded interviews and the generation of interview-derived profile images required Mercor and or its vendors to capture, extract, create, store, or use facial geometry, facial templates, faceprints, voiceprints, or other biometric identifiers or biometric information.

83. Mercor did not provide an Illinois-compliant notice explaining that artificial intelligence would analyze recorded video interviews, how the AI worked, what general characteristics it used to evaluate applicants, or which entities would receive or analyze applicant videos.

84. Mercor also did not obtain the written release required before collecting or otherwise obtaining biometric identifiers or biometric information from Illinois residents, nor did it make publicly available a retention schedule and guidelines for permanently destroying such data once the purpose of collection had been satisfied.

85. Mercor further failed to provide reliable deletion assurances even when applicants sought deletion. Ananthula never received proof that his AI interview and algorithmic analysis had been deleted. Upon information and belief, Mercor likewise failed to delete or instruct third parties to delete applicant videos and derivative materials, including biometric information, within the time required after deletion requests.

86. Upon information and belief, Mercor disclosed or made available applicants' and workers' video interviews, interview-derived images, transcripts, or biometric derivatives to vendors and Doe AI Lab Defendants beyond what was permitted or reasonably disclosed.

87. For Illinois applicants and workers, these obligations were cumulative. Mercor's duties under the Artificial Intelligence Video Interview Act did not displace its independent duties under the Illinois Biometric Information Privacy Act.

88. These practices invaded protected privacy interests independent of the later breach. The breach merely heightened the risks by exposing data that should never have been collected, retained, reused, or disclosed in the first place.

89. Moreover, these data collection practices made it foreseeable that a data breach would cause serious harm to Mercor's applicants and workers.

90. That foreseeable harmed materialized. The information compromised in the Breach included "facial biometric data used for identity matching."[10]

D. Mercor Turned Screenshots and Monitoring Artifacts into a De Facto HR File that Workers Could Not Review or Correct.

91. Mercor required at least some workers to install Insightful, a monitoring and time-tracking application, on their personal computers as a condition of continuing work. Mercor did not provide separate work devices.

92. Workers were not meaningfully informed that Insightful would capture activity beyond Mercor-specific tasks or that it could reveal personal banking, health, legal, or family information simply because the worker was using a personal device.

93. Plaintiff Bevvino-Berv exported records showing that, over the relevant monitoring period, Insightful captured activity across at least 240 distinct applications and websites, many unrelated to Mercor work.

94. Those captured activities included logins to personal bank accounts, health-insurance portals, telehealth platforms, Google Photos, personal email, utility accounts, and other private websites and applications.

95. Mercor also integrated Bevvino-Berv's personal AI account into his workflow by requiring him to use it for automated quality checks while work

[10] *Mercor Breach Exposes 4TB of Data Including Biometrics and Source* Code, AI PRODUCTIVITY (Apr. 3, 2026), https://aiproductivity.ai/news/mercor-breach-4tb-data-biometrics-source-code/.

monitoring remained active. As a result, personal, non-work conversations about legal and medical matters were exposed to Mercor's surveillance environment during work sessions.

96. Upon information and belief, Mercor stored or had access to screenshots, browser URLs, window titles, app-usage logs, time logs, IP-address data, device identifiers, and deduction records tied to monitored work sessions.

97. The data captured through Insightful and related tools revealed far more than work performance. It created a granular map of workers' private lives, including their financial institutions, health providers, telehealth usage, legal matters, and daily patterns of activity.

98. Upon information and belief, Insightful or similar monitoring tools captured screenshots at frequent intervals, including intervals as frequent as approximately every 30 to 60 seconds. A worker could not reliably know which screen moments were captured, retained, reviewed, associated with performance, disclosed to clients, or exposed in the breach.

99. These screenshots and metadata did not merely measure time. They created a record that could be read as evidence of a worker's diligence, attention, competence, discretion, loyalties, health, finances, legal problems, family life, or personal habits—even where the screenshot was accidental, misleading, out of context, or unrelated to work.

100. Mercor provided no meaningful process for workers to review that record, correct inaccurate entries, dispute false or misleading inferences, segregate non-work information, challenge client feedback, attach explanatory context, or request deletion of personal screenshots and monitoring artifacts.

101. By assembling screenshots, browser URLs, app usage, review notes, time deductions, work product, and client evaluations into a de facto HR file, Mercor and the Doe AI Lab Defendants created a due-process-like fairness problem in the

private labor market: workers were judged by a secret record they could not see, contest, or correct.

102. Once that record was stolen or exposed, the harm can become career-long. A leaked screenshot of a medical portal, legal matter, bank account, personal photo, unrelated confidential file, or embarrassing website can be copied, resold, resurfaced, or mischaracterized long after the work session ended.

103. Mercor's surveillance was particularly offensive because it occurred on workers' personal devices, without separate work hardware, without meaningful narrowing to work-only activity, and in a context where Mercor had already implied limited supervision consistent with independent-contractor status.

104. Upon information and belief, the Doe AI Lab Defendants knew or should have known that the data and work product they obtained through Mercor's pipeline was shaped by or accompanied by monitoring records, screenshots, work-session metadata, and private screen-capture data.

E. Mercor Encouraged or Tolerated Use of Source-Specific Information of Questionable Provenance While Failing to Implement Meaningful Guardrails.

105. Mercor did not simply collect information generated wholly within its own platform. It encouraged or tolerated the use of real-world source material, real experiences, and source-specific detail in worker outputs.

106. In related engagements, project managers told Plaintiff Srinarmwong and other workers that using real-life data or real experiences from their firms was encouraged so long as identifying details were redacted or slightly changed.

107. When workers attempted to protect or anonymize confidential or regulated information by writing at a higher level, Mercor reviewers criticized the work as too short and too vague and required rewrites, thereby pressuring workers to provide more source-specific detail.

108. Mercor provided no meaningful mandatory training on how to avoid disclosure of confidential, proprietary, regulated, privileged, patient-specific, or otherwise restricted information. At most, workers were left with non-mandatory documents, spreadsheets of best practices, or subjective reviewer comments.

109. Plaintiff Schenck experienced the same pressure in the applicant pipeline. In connection with a Mercor work assessment, she was instructed, in substance, to create a realistic task or case study-type scenario drawn from her area of professional expertise and to submit associated materials including a prompt, an ideal response, and a detailed scoring rubric with numerous binary criteria. She also understood the assessment to require at least one image necessary to answer the prompt and to call for source materials the type a professional would reasonably consult in that setting, including links and/or PDFs. Because her principal expertise is in clinical microbiology, she reasonably understood the assessment to require her to simulate a real professional workflow in that field. Schenck reasonably believed that completing the assessment as requested risked requiring the use of restricted, non-public, professionally controlled, or otherwise sensitive materials, creating legal and ethical concerns that made her uncomfortable completing the assignment in the manner requested.

110. Plaintiff Srinarmwong also observed numerous tasks that matched third-party online materials, including Stack Overflow questions and other public-source content, reinforcing his understanding that Mercor expected workers to draw from real-world material and was willing to blur provenance boundaries so long as output quality met client expectations.

111. Bevvino-Berv observed a related pattern in finance tasks. Based on his institutional-finance experience, he saw financial models and prompts with unusual specificity, pre-project metadata, hidden defined names, institutional data-terminal markers, real lender or counterparty names, irregular numeric precision, and other features that raised serious provenance questions.

112. For example, Bevvino-Berv observed tasks and files involving project-finance, airport, resort-development, midstream-energy, and fuel-cell modeling that included markers associated with real financial institutions or data vendors, real or apparently real asset names, real lenders or counterparties, creation dates predating the assignment, and metadata suggesting that at least some files may have been adapted from preexisting source material rather than created from scratch.

113. Mercor's own anonymization guidance reinforced the concern. Workers were instructed to remove or avoid visible company names, fund names, client names, deal names, ticker symbols, and named ranges inherited from sources and QA checklists instructed reviewers to clean named ranges. However, time constraints and other pressure Mercor put on workers made such anonymization impracticable at best.[11]

114. Mercor and the Doe AI Lab Defendants operated a system in which source files and source-specific information of uncertain origin could enter the platform, be partially anonymized at the surface, be captured by screenshots before or during anonymization, and then become part of a worker's de facto HR file and the stolen breach corpus.

115. Even if a file or screenshot ultimately reflects lawful material, it may still be misleading, personal, confidential, or professionally harmful if stored without context, associated with a worker's name, reviewed by a client, or leaked without a process for correction or explanation.

116. Upon information and belief, Mercor and the Doe AI Lab Defendants benefited from this provenance-blind pipeline by obtaining outputs, annotations, evaluations, rubrics, and training material rooted in source-specific data while avoiding adequate source-rights, provenance, privacy, and correction safeguards.

[11] At this time, Plaintiffs cannot confirm that any particular third party's trade secret was definitively stolen or that any anyone knowingly submitted stolen material.

F. Mercor and the Doe AI Lab Defendants Procured or Used Third-Party Background Reports and Algorithmic Dossiers for Work Decisions Without Complying with the FCRA.

117. Mercor required or procured third-party background checks as part of onboarding and assignment decisions. Bevvino-Berv underwent a background check administered through Certn or Zinc before beginning paid work. Crenshaw likewise completed a background check as part of her Mercor onboarding.

118. Upon information and belief, Mercor and the Doe AI Lab Defendants procured or caused to be procured background reports, identity-verification reports, algorithmic scores, interview reports, or other consumer reports bearing on applicants' and workers' character, general reputation, personal characteristics, mode of living, identity, or fitness for work from third-party reporting companies for employment or employment-like purposes.

119. Upon information and belief, the Doe AI Lab Defendants used Mercor as an intermediary to obtain or benefit from such reports, scores, dossiers, or derivative eligibility determinations, including by requiring Mercor-screened candidates, receiving client-facing shortlists, reviewing work-trial outputs, participating in interviews, and determining whether workers would be staffed or retained.

120. Upon information and belief, Defendants did not provide a clear and conspicuous stand-alone disclosure, in a document that consisted solely of the disclosure, before procuring such reports. Instead, report procurement was bundled with onboarding paperwork, offer materials, IP assignments, platform terms, or other application and engagement documents.

121. Upon information and belief, Defendants also failed in many instances to provide copies of consumer reports and summaries of rights before taking adverse action or declining to advance applicants or workers based in whole or in part on third-party reports, scores, dossiers, or derivative assessments.

122. The Consumer Financial Protection Bureau ("CFPB") has explained that employers may not use third-party background dossiers and algorithmic scores for hiring, promotion, retention, or other work decisions without complying with the FCRA's disclosure, authorization, and adverse-action requirements.[12]

123. Mercor's system did not provide the procedural protections required by the FCRA: Notice that a report will be used; authorization; a copy of the report before adverse action; a summary of rights; and a chance to identify and dispute inaccuracies before a work opportunity is lost.

124. Defendants' AI-mediated screening, client interviews, background checks, and monitoring-derived HR files created precisely the kind of opaque work-decision process in which inaccurate, misleading, or out-of-context records can deny opportunities without the worker ever learning what happened.

G. The Data Breach was the Foreseeable Result of a Fragile AI Infrastructure and False Compliance Signaling.

125. Mercor publicly represented that it used appropriate technical and organizational measures to protect personal information and publicly advertised security controls and SOC 2 Type 2 compliance.

126. But this Data Breach did not occur in isolation. It arose in a fast-moving AI infrastructure environment that rewarded speed, scale, and marketing over hardened security, dependency integrity, secrets management, and supply-chain controls.

127. Malicious versions of LiteLLM were published in March 2026 and reportedly contained malware designed to harvest environment variables, SSH keys,

[12] *See* Consumer Fin. Prot. Bureau, Circular 2024-06, *Background Dossiers and Algorithmic Scores for Hiring, Promotion, and Other Employment Decisions* (Oct. 24, 2024); Fed. Trade Comm'n, *Using Consumer Reports: What Employers Need to Know,* https://www.ftc.gov/business-guidance/resources/using-consumer-reports-what-employers-need-know (last visited Apr. 21, 2026).

cloud credentials, Kubernetes tokens, and database passwords—the kinds of secrets that can unlock access to a company's systems and data.

128. Public reporting also indicates that LiteLLM had previously obtained compliance certification through Delve and later moved away from Delve after the incident.

129. Delve marketed itself as a compliance automation company capable of obtaining certifications far faster than ordinary processes. Public reporting in March 2026 accused Delve of using fake evidence and rubber-stamped compliance materials to tell customers they were compliant without adequate investigation.

130. Upon information and belief, Mercor chose to ingest, retain, and continue using highly sensitive applicant and worker data at scale while relying on upstream AI tooling, vendors, and compliance signaling that were not secured or validated to the degree such data demanded.

131. Mercor's choice to centralize full HR files, interview data, background data, payment records, monitoring logs, and other sensitive material while relying on such a brittle stack made the breach foreseeable.

H. Mercor Confirmed the Occurrence of the Data Breach but Withheld the Full Truth about its Scope.

132. On March 31, 2026, Mercor notified Plaintiffs and other affected persons of a security incident. The notice did not identify the attack, specify the categories of data implicated, explain what steps affected persons should take, or offer credit monitoring or identity-theft protection.

133. Mercor stated only that there had been a recent security incident affecting its systems and thousands of other organizations, that it had secured its systems, and that a third-party forensic investigation was ongoing.

134. Mercor has still not publicly identified all affected systems, all affected individuals, all affected categories of data, the duration of unauthorized access,

whether interview videos and transcripts were exfiltrated, whether monitoring data and screenshots were exposed, whether tax and payment materials were implicated, whether background-check or identity-verification records were compromised, whether source-adjacent files or work-product repositories were exposed, or whether the stolen information has already been misused.

135. Public reporting indicates that sample data allegedly taken from Mercor included Slack-related material, ticketing data, and videos purportedly showing conversations between Mercor's AI systems and contractors.

136. Public reporting indicated three general types of data were exfiltrated:

- Candidate records (211GB): Resumes, verified contact information, and Social Security numbers from people who applied through Mercor's platform.
- Video and identity verification (3TB): High-definition recordings of candidate interviews, passport and driver's license scans, and facial biometric data used for identity matching. This is the bulk of the stolen data and by far the most sensitive.
- Source code (939GB): Mercor's proprietary matching algorithms, internal dashboards, benchmarking code, and—critically—hardcoded API keys that could give attackers further access to Mercor's cloud systems.[13]

137. Upon information and belief, that public reporting was originally derived from claims the hackers made on the dark web about the extent of the data they had exfiltrated.

138. Publicly available analyses of allegedly exfiltrated files further describe data structures reflecting bank-routing data, payment-account identifiers, government-ID-verification records, signed legal documents, direct URLs for contractor screenshots, and references to storage locations for AI interview recordings, background-check photographs, and monitoring screenshots.

139. These categories are consistent with Mercor's business model and the data Plaintiffs and class members were required to provide.

[13] AI PRODUCTIVITY, *supra* note 4.

140. What was exposed, therefore, was not merely basic contact information. It was the functional equivalent of complete HR files for applicants and workers, plus surveillance records gathered from personal devices and source-adjacent work records that workers could not review or correct.

I. Plaintiffs Have Suffered Concrete and Continuing Harm.

141. Ananthula has suffered actual and ongoing harm because Mercor has never confirmed deletion of his AI interview or associated algorithmic analysis. He now faces continuing risks of impersonation, deepfake misuse, and long-term retention and reuse of his interview data.

142. Schenck has suffered actual and ongoing harm from the exposure of her financial, identity, interview, and work-trial data, as well as from the unauthorized or inadequately disclosed use of her interview imagery to generate a profile picture. After the breach, she experienced suspicious account activity, changed passwords, and locked her credit.

143. Crenshaw has suffered actual and ongoing harm from the exposure of her identity, background check, payment, interview, and project data, as well as from the collection and use of her biometric data without the notices and consents required by Illinois law. She later experienced unauthorized account activity and spam calls.

144. Srinarmwong has suffered actual and ongoing harm because Mercor retained and exposed contractor-specific data associated with his projects, communications, work product, and project-related expectations regarding real-world source material, creating continuing risks of professional harm, confidentiality breaches, and reputational damage.

145. Bevvino-Berv has suffered actual and ongoing harm from the exposure or threatened exposure of his full contractor record, including tax-identification information, government identification, banking details, resume, professional credentials, interview and background-check records, Insightful app and website usage, personal banking and health-portal activity, telehealth usage, legal-research

activity, personal AI account usage, and work-product and reviewer records tied to a client AI lab project.

146. Bevvino-Berv is particularly concerned that records reflecting Mercor and AI lab performance assessments, project-status changes, quality-assurance materials, audit-related records, and monitoring artifacts whose meaning he cannot inspect, correct, or contextualize.

147. Plaintiffs have spent and will continue to spend time mitigating the consequences of Defendants' conduct, including securing accounts, monitoring for fraud, reviewing records, and investigating what happened.

148. Plaintiffs would not have provided the same scope or quantity of sensitive information, would not have done so on the same terms, and would not have participated in Mercor's AI-driven screening, source-material, and monitoring system as they did had they known the truth about Defendants' collection, retention, sharing, surveillance, biometric, consumer-reporting, source-provenance, correction, and security practices.

CLASS ALLEGATIONS

149. Plaintiffs bring this action pursuant to Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of themselves and the following proposed classes and subclasses:

Nationwide Class

All natural persons in the United States whose personal information, interview data, screening data, background-check data, monitoring data, work-product data, or related records were collected, maintained, processed, stored, or used by Mercor and were accessed, exfiltrated, stolen, disclosed, or reasonably believed to have been accessed, exfiltrated, stolen, or disclosed in connection with the March 2026 Mercor incident.

Applicant Subclass

All members of the Nationwide Class who applied for work through Mercor and completed one or more AI interviews, recorded interviews, assessments, work trials, identity-verification steps, or background-screening steps.

Worker Subclass

All members of the Nationwide Class who accepted Mercor work or performed services through Mercor and whose work sessions, computer activity,

screenshots, app usage, browser activity, window titles, time logs, deductions, work-product records, review notes, client feedback, or similar records were captured, stored, used, or exposed by Insightful or similar monitoring or worker-management tools.

Illinois Biometric Subclass

All Illinois residents whose biometric identifiers or biometric information were collected, captured, purchased, received through trade, or otherwise obtained, stored, used, disclosed, redisclosed, or transmitted by Mercor or the Doe AI Lab Defendants through AI interviews, interview-derived images, profile-photo generation, or related processes.

Illinois Video Interview Subclass

All persons residing in Illinois or who submitted recorded video interviews for positions based in Illinois and whose videos were analyzed by artificial intelligence or shared or retained in violation of the Artificial Intelligence Video Interview Act.

FCRA Subclass

All natural persons in the United States about whom Mercor, the Doe AI Lab Defendants, or any person acting on their behalf procured, caused to be procured, used, or received a background report, consumer report, identity-verification report, algorithmic score, interview report, or other third-party background dossier for employment or employment-like purposes in connection with an application, offer, onboarding, assignment, reassignment, routing, retention, continuation, or removal decision.

Florida Consumer Subclass

All members of the Nationwide Class who reside in Florida or resided in Florida at the time they applied for or performed work through Mercor and provided personal information, interview data, work-trial data, monitoring data, or labor through Mercor's platform.

150. Plaintiffs reserve the right to amend, narrow, expand, or refine these definitions as discovery and investigation progress.

151. Excluded from the Classes are Defendants; Defendants' officers, directors, parents, subsidiaries, and affiliates; Plaintiffs' and Defendants' inside and outside legal counsel; the Court and its staff; and any judge assigned to this case and that judge's immediate family.

152. Numerosity is satisfied because Mercor publicly acknowledged that it was among thousands of firms affected by the LiteLLM compromise, Mercor operates at scale, and the platform collected data from large numbers of applicants and

workers. Upon information and belief, the Data Breach resulted in the exposure of millions of victims' PII and/or PHI.

153. Common questions of law and fact include, without limitation: (a) what categories of data Mercor and the other Defendants collected, processed, stored, reused, disclosed, or exposed; (b) whether Mercor and the Doe AI Lab Defendants used AI interviews, automated scoring, background screening, and direct-client review to make or inform hiring, matching, routing, assignment, retention, audit, or continuation decisions; (c) whether Mercor and the Doe AI Lab Defendants acted as employers, joint employers, employment agencies, agents, users of consumer reports, or users of screening tools within the meaning of applicable law; (d) whether Defendants failed to implement reasonable data-security, retention, deletion, vendor-management, provenance, and monitoring safeguards; (e) whether Defendants collected, stored, or disclosed biometric identifiers or biometric information without the notices, consent, retention schedules, and limitations required by Illinois law; (f) whether Defendants procured, caused to be procured, used, or received consumer reports without the disclosures, authorizations, certifications, and notices required by the FCRA; (g) whether Mercor's monitoring of workers' personal devices intruded upon private affairs in a manner highly offensive to a reasonable person; (h) whether Defendants created de facto HR files without meaningful access, correction, or dispute procedures; (i) whether Defendants misrepresented or omitted material facts about AI screening, biometric processing, surveillance, background checks, source-provenance controls, deletion, correction, and security practices; (j) whether Plaintiffs and class members suffered legally cognizable injury and damages; and (k) whether Plaintiffs and the Classes are entitled to damages, statutory damages, restitution, declaratory relief, injunctive relief, or other relief.

154. Plaintiffs' claims are typical of the claims of the Classes because their claims arise from the same course of conduct and are based on the same legal theories.

155. Plaintiffs will fairly and adequately represent the Classes. They have no conflicts with the Classes and have retained counsel experienced in complex litigation, privacy litigation, class actions, and technology-related disputes.

156. Class treatment is appropriate because common questions predominate over individual issues and because a class action is superior to individual litigation given the number of affected persons and the relatively modest size of many individual claims compared with the complexity and cost of litigating them separately.

157. Injunctive and declaratory relief are appropriate because Defendants continue to retain interview data, biometric data, monitoring records, background data, source-adjacent work records, screenshots, and other sensitive information; the full scope of the incident remains unknown; and Defendants' ongoing hiring, screening, surveillance, retention, deletion, notice, correction, and FCRA practices are capable of class-wide adjudication.

CAUSES OF ACTION

COUNT I

Negligence

(On Behalf of Plaintiffs and the Nationwide Class Against All Defendants)

158. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

159. Mercor owed Plaintiffs and the Class a duty to exercise reasonable care in collecting, processing, storing, securing, retaining, using, correcting, and protecting their personal information, interview data, screening data, background data, monitoring data, source-adjacent records, and other sensitive records.

160. Delve and LiteLLM, as upstream providers whose conduct and representations foreseeably affected the security of Mercor's systems, also owed duties of reasonable care not to create or misrepresent security conditions in a manner that foreseeably exposed Plaintiffs' data to compromise.

161. Mercor and the Doe AI Lab Defendants likewise owed duties of reasonable care in connection with the AI-driven screening, collection, disclosure, retention, source-provenance, correction, and use of applicants' and workers' data, including data they required as a condition of access to work.

162. Defendants breached these duties by, among other things, failing to implement and maintain reasonable security safeguards; failing to adequately manage and harden dependencies and vendors; failing to minimize retention; failing to protect credentials and secrets; failing to segment sensitive systems; collecting and retaining more data than necessary; failing to distinguish work and non-work monitoring records; failing to implement reasonable source-provenance controls; failing to provide meaningful access and correction processes for de facto HR files; disclosing or reusing interview, screening, biometric, and monitoring data without adequate safeguards; and failing to timely and fully notify affected persons of the nature and scope of the incident.

163. The harms that occurred here were foreseeable. Defendants concentrated unusually sensitive applicant and worker data in a platform built on fast-moving AI infrastructure while using opaque screening, monitoring, and data-retention practices that increased both the amount of harm and the likelihood of misuse if the system failed.

164. As a direct and proximate result of Defendants' negligence, Plaintiffs and class members suffered loss of privacy, increased risk of identity theft and fraud, mitigation expenses, emotional distress, professional harm, diminished value of their data, lost income, and ongoing risk associated with retention and reuse of their interview, biometric, background, monitoring, and source-adjacent records.

165. Defendants' conduct was intentional, willful and wanton, reckless, and/or grossly negligent, entitling Plaintiffs and the Class to punitive damages.

COUNT II

Breach of Implied Contract

(On Behalf of Plaintiffs and the Nationwide Class Against Mercor)

166. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

167. Plaintiffs and class members entered into implied contracts with Mercor under which Mercor accepted valuable consideration—including personal information, interview participation, work-trial participation, background-screening participation, labor availability, platform participation, monitoring compliance, and work product—in exchange for providing work-matching, screening, worker-management, and related services while using reasonable measures to safeguard the information entrusted to it and handling that information consistently with its disclosures.

168. Those implied contracts included, at minimum, promises that Mercor would not collect, retain, reuse, disclose, expose, or silently convert applicants' and workers' data into inaccessible de facto HR files in ways materially inconsistent with reasonable expectations created by Mercor's privacy, security, platform, and independent-contractor representations.

169. Plaintiffs and class members performed by providing the requested information, completing interviews and work trials, participating on the platform, installing required monitoring tools, and providing labor or availability.

170. Mercor breached the implied contracts by failing to use reasonable measures to protect Plaintiffs' and class members' information, by failing to adequately disclose and limit AI screening, biometric processing, background check, source-provenance, and surveillance practices, by failing to provide meaningful access and correction procedures for de facto HR files, and by failing to adequately secure the systems through which that information was collected and exposed.

171. As a direct and proximate result of Mercor's breaches, Plaintiffs and class members suffered damages in an amount to be proven at trial.

172. Defendants' conduct was intentional, willful and wanton, reckless, and/or grossly negligent, entitling Plaintiffs and the Class to punitive damages.

COUNT III

Intrusion Upon Seclusion

(On Behalf of Plaintiffs and the Worker Subclass Against Mercor and the Doe AI Lab Defendants)

173. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

174. Plaintiffs and members of the Worker Surveillance and Effective HR File Subclass had a reasonable expectation of privacy in the contents of their personal computers, their personal bank and insurance portals, telehealth sessions, personal email, personal legal and family-related communications, private photographs, intimate or embarrassing browsing activity, and other private activity unrelated to Mercor work.

175. Mercor intentionally intruded upon that seclusion by requiring workers to install Insightful or similar software on personal devices, capturing screenshots and usage data far beyond the scope of any legitimate work need, retaining or transmitting that data, and converting it into a worker-management and de facto HR record.

176. Upon information and belief, the Doe AI Lab Defendants intentionally benefited from, directed, approved, or participated in this intrusion by receiving, using, requiring, or relying on data, reports, work product, audits, or staffing decisions generated through surveillance practices they knew or should have known extended beyond legitimate work monitoring and swept in private information.

177. These intrusions would be highly offensive to a reasonable person.

178. As a direct and proximate result, Plaintiffs and class members suffered loss of privacy, emotional distress, and other damages.

179. Defendants' conduct was intentional, willful and wanton, reckless, and/or grossly negligent, entitling Plaintiffs and the Class to punitive damages.

COUNT IV

Violation of the Fair Credit Reporting Act

(15 U.S.C. § 1681b(b)) (On Behalf of Plaintiffs and the FCRA Subclass Against Mercor and the Doe AI Lab Defendants)

180. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

181. Mercor and, upon information and belief, the Doe AI Lab Defendants procured, caused to be procured, used, received, or benefited from consumer reports, background reports, identity-verification reports, algorithmic scores, interview reports, or other third-party background dossiers for employment or employment-like purposes in connection with hiring, onboarding, assignment, routing, reassignment, continuation, retention, audit, and removal decisions.

182. Consumer reports for employment purposes include background dossiers and, when furnished by a third party for hiring or retention decisions, algorithmic scores and similar reports bearing on a consumer's character, general reputation, personal characteristics, mode of living, or fitness for work.

183. The Doe AI Lab Defendants cannot avoid FCRA duties by routing screening through Mercor. Upon information and belief, Mercor acted as their agent or intermediary, procured reports for their benefit, furnished or transmitted eligibility determinations, and provided shortlists, interview access, work-trial outputs, background-screened candidates, or continuation decisions shaped by third-party reports or scores.

184. Before procuring such reports, Defendants were required to provide a clear and conspicuous disclosure in writing, in a document consisting solely of the disclosure, that a consumer report might be obtained for employment purposes, and to obtain written authorization from the consumer. 15 U.S.C. section 1681b(b)(2)(A).

185. Upon information and belief, Defendants failed to provide the required stand-alone disclosures and/or failed to obtain legally sufficient written authorizations

before procuring such reports. Instead, report procurement was bundled with other onboarding, application, offer, IP-assignment, or platform materials.

186. Upon information and belief, when Defendants took adverse action based in whole or in part on such reports, scores, dossiers, or derivative eligibility decisions, they also failed to provide required pre-adverse-action and adverse-action notices, including copies of reports and summaries of rights, as required by 15 U.S.C. section 1681b(b)(3).

187. These violations were willful, and in the alternative negligent.

188. Plaintiffs and members of the FCRA Subclass are entitled to actual damages, statutory damages, punitive damages to the extent allowed, costs, attorneys' fees, and all other relief authorized by the FCRA.

COUNT V

Violation of the Illinois Biometric Information Privacy Act

(740 ILCS 14/15(a), 15(b), and 15(d)) (On Behalf of Crystal Crenshaw and the Illinois Biometric Subclass Against Mercor and the Doe AI Lab Defendants)

189. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

190. Mercor and, upon information and belief, the Doe AI Lab Defendants collected, captured, stored, used, received through trade, or otherwise obtained biometric identifiers or biometric information from Illinois residents, including facial geometry, face templates, faceprints, voiceprints, or other biometric derivatives extracted from recorded video interviews and interview-derived imagery.

191. Defendants failed to develop, make publicly available, and comply with a written policy establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collection had been satisfied or within the time required by law, in violation of section 15(a).

192. Defendants collected, captured, or otherwise obtained Illinois residents' biometric identifiers or biometric information without first informing them in writing

that such data was being collected or stored, informing them in writing of the specific purpose and length of term for which it was being collected, stored, and used, and obtaining a written release, in violation of section 15(b).

193. Defendants disclosed, redisclosed, or otherwise disseminated biometric identifiers or biometric information to vendors, platform partners, or Doe AI Lab Defendants without the consent required by law and outside the limited circumstances permitted by section 15(d).

194. Crenshaw and members of the Illinois Biometric Subclass suffered an invasion of their statutory and privacy rights the moment Defendants collected, retained, used, or disclosed their biometric data without complying with BIPA.

195. Crenshaw and the Illinois Biometric Subclass seek all relief available under BIPA, including liquidated damages, injunctive relief, attorneys' fees, costs, and any other relief the Court deems appropriate.

COUNT VI

Violation of the Illinois Artificial Intelligence Video Interview Act

(820 ILCS 42/5, 10, 15, and 20) (On Behalf of Crystal Crenshaw and the Illinois Video Interview Subclass Against Mercor and the Doe AI Lab Defendants)

196. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

197. Mercor and, upon information and belief, the Doe AI Lab Defendants asked applicants to record video interviews and used artificial intelligence analysis of applicant-submitted videos in considering applicants for positions involving Illinois residents and for positions based in Illinois.

198. Before asking applicants to submit video interviews, Defendants did not provide the notices, explanations, and consent procedures required by section 5 of the Act, including notice that AI would analyze the interview, an explanation of how the AI worked and what general types of characteristics it used, and valid consent to AI evaluation.

199. Defendants shared or made available applicant videos more broadly than permitted by section 10 and failed to ensure timely deletion and downstream deletion upon request as required by section 15.

200. Upon information and belief, Defendants also failed to collect and report demographic data as required when relying solely on AI analysis to determine whether an applicant would be selected for an in-person interview.

201. Crenshaw and members of the Illinois Video Interview Subclass seek all relief available at law or in equity, including declaratory and injunctive relief, restitution, damages to the extent authorized, and use of AIVIA violations as unlawful or unfair predicates for related statutory and equitable claims.

COUNT VII

Violation of the Illinois Consumer Fraud and Deceptive Business Practices Act

(815 ILCS 505/2) (On Behalf of Crystal Crenshaw and the Illinois Subclasses Against Mercor)

202. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

203. Crenshaw and members of the Illinois subclasses were consumers within the meaning of the Act because they sought and acquired work-matching, screening, or platform services from Mercor and provided valuable personal data and participation as consideration.

204. Mercor engaged in deceptive and unfair acts or practices by representing or implying that it used lawful, transparent, and appropriately limited AI screening, biometric processing, background-check, deletion, correction, monitoring, source-provenance, and data-security practices while failing to disclose material facts concerning those practices.

205. Among other things, Mercor failed to disclose that it would use or cause the use of AI to analyze recorded interviews; generate or offer profile images from interview-derived facial imagery; retain and reuse interview results across applications; procure or use third-party background reports without legally adequate

stand-alone disclosures; surveil workers' personal devices through software that captured private, non-work activity; convert monitoring artifacts into de facto HR files without access or correction procedures; and retain, share, or fail to timely delete applicant videos and related data in ways inconsistent with Illinois law.

206. These omissions and misrepresentations were material and were intended to induce applicants and workers, including Crenshaw, to participate in Mercor's platform and surrender valuable personal data and labor.

207. Crenshaw and members of the Illinois subclasses suffered actual damages as a result.

208. Mercor's conduct was unfair because the injury to consumers and workers outweighed any countervailing benefits and offended established public policy reflected in Illinois privacy, biometric, video-interview, consumer-protection, and employment statutes.

209. Crenshaw and the Illinois subclasses seek actual damages, punitive damages where available, restitution, injunctive relief, attorneys' fees, and all other appropriate relief.

COUNT VIII

Violation of the Florida Deceptive and Unfair Trade Practices Act

(Fla. Stat. §§ 501.201 et seq.) (On Behalf of Calista Schenck, David Bevvino-Berv, and the Florida Consumer Subclass Against Mercor and the Doe AI Lab Defendants)

210. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

211. Schenck, Bevvino-Berv, and members of the Florida Consumer Subclass were consumers or persons injured by unfair or deceptive acts or practices in trade or commerce because they sought and acquired work-matching, screening, AI-interview, project-access, or platform services from Mercor and provided valuable personal data, interview participation, monitoring compliance, work-trial materials, and labor or labor availability as consideration.

212. Mercor and, upon information and belief, the Doe AI Lab Defendants engaged in deceptive and unfair acts or practices by misrepresenting or omitting material facts regarding AI screening, direct-client decision-making, background-check procurement, consumer-report use, worker surveillance, source-provenance controls, de facto HR files, access and correction rights, data security, breach scope, and remediation.

213. The conduct was deceptive because reasonable applicants and workers in Florida would have considered it material that Defendants would capture, retain, reuse, and expose interview data, tax and banking data, background-screening data, screenshots, app and website usage, client evaluations, and source-adjacent work records without meaningful transparency or correction procedures.

214. The conduct was unfair because it caused substantial injury to Florida applicants and workers that they could not reasonably avoid, including loss of privacy, mitigation costs, lost time, emotional distress, professional risk, lost work opportunities, and exposure of de facto HR files that may follow them throughout their careers.

215. Schenck, Bevvino-Berv, and the Florida Consumer Subclass suffered actual damages and are entitled to damages, declaratory relief, injunctive relief, attorneys' fees, costs, and all other relief permitted by FDUTPA.

COUNT IX

Unjust Enrichment

(Against All Defendants, in the Alternative)

216. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

217. Defendants received and retained benefits from Plaintiffs and class members, including valuable personal data, biometric data, interview data, work-trial data, monitoring data, source-adjacent work records, and labor, which Defendants used to operate, market, and profit from their platform, screening systems, projects, and AI-development activities.

218. It would be unjust for Defendants to retain those benefits while avoiding the costs of lawful disclosures, lawful consents, reasonable security, lawful retention and deletion, source-provenance safeguards, meaningful access and correction procedures, and lawful screening and monitoring practices.

219. Plaintiffs and class members are entitled to restitution, disgorgement, and all other equitable relief available.

COUNT X

Declaratory and Injunctive Relief

(On Behalf of Plaintiffs and the Classes Against All Defendants)

220. Plaintiffs incorporate all preceding paragraphs as if fully set forth herein.

221. An actual controversy exists regarding whether Defendants' current and ongoing practices concerning AI screening, biometric processing, background-check procurement, consumer-report use, surveillance, source-provenance controls, de facto HR files, retention, deletion, sharing, correction, and data security comply with applicable law.

222. Plaintiffs and class members face continuing risk because Defendants continue to retain their interview data, biometric data, monitoring records, background data, source-adjacent work records, screenshots, review notes, client feedback, and other sensitive information, while the full scope of the breach and the full universe of downstream recipients remain unknown.

223. Plaintiffs and class members seek declaratory and injunctive relief requiring Defendants to, among other things: (a) identify and disclose all categories of data affected by the March 2026 incident; (b) identify all downstream recipients of interview data, biometric data, background reports, monitoring data, source-adjacent records, and de facto HR file materials; (c) provide complete and accurate notice to affected persons; (d) provide credit monitoring, identity-theft protection, fraud monitoring, tax-fraud monitoring, and related remediation; (e) delete interview videos, biometric derivatives, monitoring records, screenshots, and source-adjacent

records not lawfully retained, and instruct downstream recipients to do the same; (f) publish and implement compliant biometric-retention and destruction policies; (g) cease using AI video analysis without legally required notice, explanation, consent, and deletion procedures; (h) cease procuring, causing to be procured, or using consumer reports without FCRA-compliant disclosures, authorizations, certifications, notices, and adverse-action procedures; (i) cease monitoring workers on personal devices without meaningful, lawful, and narrowly tailored limitations; (j) create a process for applicants and workers to access, correct, dispute, contextualize, and request deletion of their de facto HR files, including screenshots, monitoring logs, review notes, client feedback, and algorithmic assessments; (k) submit to independent security, privacy, provenance, FCRA, and algorithmic-impact audits, including audits for adverse impact in screening and selection; (l) provide meaningful human review and challenge procedures for AI-mediated screening and adverse decisions; and (m) provide such other equitable relief as the Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Classes, respectfully request that the Court enter judgment in their favor and against Defendants as follows:

A. Certifying this action under Rule 23, appointing Plaintiffs as class representatives, and appointing their counsel as class counsel;

B. Awarding actual, consequential, general, compensatory, statutory, and punitive damages as permitted by law;

C. Awarding liquidated or statutory damages under BIPA, statutory and punitive damages under the FCRA as allowed, damages and equitable relief under ICFA and FDUTPA as allowed, and all other statutory relief available;

D. Awarding restitution, disgorgement, declaratory relief, and injunctive relief;

E. Ordering Defendants to provide full and accurate notice of the incident and appropriate protective services;

F. Ordering Defendants to identify, produce, correct, delete, and remediate applicants' and workers' de facto HR files, including screenshots, monitoring artifacts, interview records, background reports, client feedback, and algorithmic assessments;

G. Awarding pre-judgment and post-judgment interest;

H. Awarding attorneys' fees, costs, and expenses as permitted by law; and

I. Granting such other and further relief as the Court deems just and proper.

JURY TRIAL DEMAND

Plaintiffs demand a trial by jury on all issues so triable.

Dated: April 21, 2026

Respectfully submitted,

/s/ Renner K. Walker
Renner K. Walker (Bar No. 295889)
HAUSFELD LLP
rwalker@hausfeld.com
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
Telephone: (646) 357-1100
Facsimile: (212) 202-4322

Steven M. Nathan (Bar No. 153250)
snathan@hausfeld.com
Jacob Leiken*
jleiken@hausfeld.com
HAUSFELD LLP
33 Whitehall Street, Fourteenth Floor
New York, NY 10004
Telephone: (646) 357-1100
Facsimile: (212) 202-4322

James J. Pizzirusso*
jpizzirusso@hausfeld.com
Ian J. Engdahl*
iengdahl@hausfeld.com
HAUSFELD LLP
1200 17th Street N.W., Suite 600
Washington, DC 20036
Telephone: (202) 540-7200
Facsimile: (202) 540-7201

Christopher L. Lebsock (Bar No. 184546)
clebsock@hausfeld.com
HAUSFELD LLP
580 California Street, 12th Floor
San Franscisco, CA 94104
Telephone: (415) 633-1908
Facsimile: (415) 633-4980

Nicholas Andrew Hall*
nhall@hallattorneys.com
HALL ATTORNEYS, P.C.
P.O. Box 1370
Edna, Texas 77957
Telephone: (713) 428-8967

Attorneys for Plaintiffs and the Putative Classes

** Pro Hac Vice forthcoming*