IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

BOBBY DEES, individually and on behalf of all others similarly situated,	)	
Plaintiff,	)	
v.	)	**CIVIL ACTION NO.: 1:26-cv-924**
AINS, LLC D/B/A OPEXUS A/K/A CASEPOINT,	)	
Defendants.	)	

CLASS ACTION COMPLAINT

Plaintiff Bobby Dees, by and through undersigned counsel, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant AINS, LLC d/b/a Opexus and Casepoint ("Defendant" or "Opexus"), and alleges the following based upon personal knowledge as to himself and his own acts, and upon information and belief as to all other matters, including the investigation of counsel.

I. INTRODUCTION

1. This is a putative class action on behalf of all persons in the United States and the State of Alabama whose personal data was exposed, compromised, accessed, copied, deleted, or otherwise mishandled as a result of grossly inadequate data security and insider access controls maintained by Defendant formerly known as AINS, LLC, doing business as Opexus and Casepoint ("Defendant" or "Opexus"),

a government technology contractor that stores, processes, and manages highly sensitive government and third-party information (including personally identifiable information ("PII")).

2. At the center of this case is Defendant's decision to entrust sensitive government systems to individuals who had previously been prosecuted and convicted by the United States Government in 2015 for federal hacking and wire-fraud offenses involving unauthorized access to government computer systems, convictions that were matters of public record well before their employment at Opexus. No reasonable government contractor exercising ordinary care would have granted privileged access to audit, investigative, or FOIA systems to individuals with known histories of hacking government networks. The risk of misuse, retaliation, or data destruction under these circumstances was not speculative, it was obvious, foreseeable, and entirely preventable through minimal due diligence.

3. As such, this was not a close call or a nuanced judgment error. It was a categorical failure to apply even the most basic principles of personnel security and risk management. By placing individuals with proven records of abusing government systems into positions of trust with internal access, Opexus effectively invited the very misconduct that ultimately occurred.

4. In February 2025, Defendant enabled these two (federally convicted) employees to use privileged access to Defendant's information systems to exfiltrate

files and delete dozens of databases containing government records, including records related to federal agencies' Freedom of Information Act requests, audits, and investigations.[1] These actions caused widespread loss, disruption, and unauthorized access to sensitive materials belonging to government agencies and potentially individuals whose data was embedded within those records.[2]

5. Defendant's insufficient background checks, inadequate access controls, and systemic security failures permitted persons with known histories of cyber offenses to access, copy, retain, and delete sensitive information.[3] Defendant's conduct was negligent, breached its contractual and common-law duties, and violated applicable data protection standards and consumer protection laws, including those of Alabama as to the subclass described below.

6. As a direct and proximate result of these security failures, Plaintiff and the Class and Subclass members have sustained and continue to face: (a) increased risk of identity theft, fraud, and misuse of their PII; (b) ascertainable losses attributable to efforts to mitigate and remediate harms; (c) deprivation of the benefit of the bargain for cybersecurity protections promised by Defendant; and (d) privacy

[1] https://www.insurancejournal.com/news/national/2025/05/21/824641.htm (Last accessed Feb. 9, 2026).
[2] https://www.adminbyrequest.com/en/blogs/government-data-wiped-by-insider-hackers-in-opexus-security-breach (Last accessed Feb. 9, 2026).
[3] https://cyberscoop.com/opexus-background-checks-insider-attack-muneeb-sohaib-akhter/ (Last accessed Feb. 9, 2026).

invasions that the law protects.

7. Plaintiff brings this action to obtain compensatory damages, statutory damages, restitution, injunctive relief, and other appropriate remedies on behalf of himself and all others similarly situated.

II. PARTIES

8. Plaintiff, Bobby Dees is a natural person over the age of 19 and a resident of the State of Alabama. Plaintiff submitted information to the Equal Employment Opportunity Commission ("EEOC") in connection with an employment-related matter and, in doing so, provided sensitive personal information, including personally identifiable information ("PII"), to the EEOC for official government purposes. The EEOC utilizes third-party contractors to store, process, and manage case files, correspondence, and electronic records associated with charges of discrimination and related enforcement activities, including information submitted by charging parties such as Plaintiff.[4] The Equal Employment Opportunity Commission is a federal agency headquartered in Washington, District of Columbia.

9. At all relevant times, Plaintiff's personal information was stored, processed, or otherwise maintained within systems operated or controlled by

[4] https://www.eeoc.gov/employers/about-eeocs-digital-charge-system (Last accessed Feb. 9, 2026).

Defendant as part of Defendant's contractual relationship with the EEOC and its provision of case-management and related services.[5]

10. Defendant formerly known as AINS, LLC d/b/a Opexus and Casepoint ("Opexus") is a limited liability company organized under the laws of the District of Columbia, with its principal place of business in Washington, D.C.

11. At all relevant times, including the time of the data breach at issue, Defendant Casepoint maintained its principal place of business in Virginia and was registered and authorized to transact business in Virginia. Casepoint merged with Defendant Opexus in January of 2025[6], with its principal place of business in Washington, D.C. Defendant Casepoint maintained substantial and continuous operations in the United States, including operations serving federal agencies headquartered in Washington, D.C.

12. Opexus is a government technology contractor that provides case-management, records-management, and compliance software solutions to federal agencies, including platforms used to process investigations, enforcement actions, audits, and Freedom of Information Act ("FOIA") requests.[7]

13. Opexus represents that it sells case-management software solutions to

[5] https://www.insurancejournal.com/news/national/2025/05/21/824641.htm). (Last accessed Feb. 9, 2026).
[6] https://www.govtech.com/biz/opexus-buys-casepoint-and-wins-big-pe-investment (Last accessed Feb. 9, 2026).
[7] https://www.opexustech.com/federal-solutions/ (Last accessed Feb. 9, 2026).

a substantial portion of the federal government and that it handles sensitive data for nearly every U.S. federal agency, including civil rights enforcement agencies.

14. Opexus has publicly stated that its platforms are "trusted by" "80%" of federal agencies, *Id.,* and are used to manage highly sensitive government data, including information relating to individuals who interact with those agencies.

15. In or around 2021, Opexus merged with Casepoint, a provider of data discovery and compliance software, further expanding its access to and control over large volumes of structured and unstructured data maintained for government clients.[8]

16. Opexus served as a contractor for the EEOC and other federal agencies at the time of the February 2025 data security incident involving unauthorized insider access, data deletion, and data exfiltration.[9]

17. Opexus is owned by a private equity firm and has received tens of millions of dollars in government contracts[10], reflecting its sophistication, resources, and responsibility to implement robust cybersecurity controls commensurate with the sensitivity of the data it maintains.

18. At all relevant times, Defendant conducted business nationwide,

[8] https://www.casepoint.com/press/opexus-casepoint-merger-and-majority-investment-from-thoma-bravo (Last accessed Feb. 9, 2026).
[9] https://databreaches.net/2026/01/08/eeoc-experienced-security-incident-involving-an-opexus-employees-unauthorized-access-email-says/ (Last accessed Feb. 9, 2026).
[10] https://financialpost.com/pmn/business-pmn/probe-found-security-lapses-led-to-us-contractors-data-breach (Last accessed Feb. 9, 2026).

including activities that caused harm to Plaintiff in Alabama, and purposefully availed itself of the privilege of conducting business involving the personal information of residents throughout the United States.

III. JURISDICTION AND VENUE

19. This Court has original jurisdiction under 28 U.S.C. § 1332(d)(2) (the Class Action Fairness Act, "CAFA") because this is a putative class action in which the aggregated amount in controversy exceeds $5,000,000.00, exclusive of interest and costs; at least one member of the proposed class is a citizen of a state different from Defendant; and the proposed class consists of more than 100 members.

20. The Court has subject-matter jurisdiction over Plaintiff's federal claims pursuant to 28 U.S.C. § 1331, and supplemental jurisdiction over Plaintiff's state-law claims pursuant to 28 U.S.C. § 1367 because they arise under laws of the United States and the rights, duties, and obligations recognized by the State of Alabama as applied to the Alabama Subclass.

21. This Court has personal jurisdiction over Defendant because Defendant maintains substantial contacts and business operations within the United States and purposefully avails itself of the judicial system of the United States. Defendant contracts with and performs professional services for federal and state government agencies, including agencies whose principal operations are in Washington, D.C.

22. Venue is proper in this District under 28 U.S.C. § 1391(b)(2) because a

substantial part of the events and omissions giving rise to the claims occurred in this District, including the harm to Plaintiff and the classes via Defendant's centralized data systems and operations. Defendant is headquartered in and provides technology services used by federal agencies headquartered in Washington, D.C.

23. Venue is also proper under 28 U.S.C. § 1391(c) because Defendant conducts business in this district and is subject to personal jurisdiction here. Venue is also proper under 28 U.S.C. § 1391(b) because Defendant conducts substantial business with federal agencies located in this District and regularly transacts business within the District of Columbia.

IV. FACTUAL ALLEGATIONS

A. Background

24. Opexus, formerly AINS, LLC, is a technology contractor that provides software and data management services to federal, state, and local governments, including platforms for processing Freedom of Information Act ("FOIA") requests and case records. Its products are used to upload, store, organize, and retain data submitted to government agencies, including personal identifying information of individuals whose records are subject to public requests or agency review.[11]

25. Defendant provides technology systems used by numerous federal

[11] https://www.bloomberg.com/news/newsletters/2025-05-21/how-2-hackers-erased-hundreds-of-foia-requests (Last accessed Feb. 9, 2026).

agencies headquartered in Washington, D.C., including systems used to manage Freedom of Information Act requests, regulatory investigations, and agency case files. These systems process and store sensitive information submitted to federal agencies located in the District of Columbia, including records maintained by the Equal Employment Opportunity Commission.

26. Opexus markets its solutions as enterprise-grade platforms that support government transparency and compliance workflows, and it asserts that its technologies serve a broad base of government clients across the United States. These clients rely on Opexus technology to handle sensitive operational data, including PII that, if exposed, could facilitate identity theft or other harms.[12]

27. Third-party data custodians like Opexus play an outsized role in modern cybersecurity landscapes because they act as trusted intermediaries between public agencies and the data those agencies hold. A breach at such a custodian can create risk exposure far beyond the contractor itself because of integrated data dependencies and privileged access rights.[13]

28. Cybersecurity research and industry reporting make clear that third-party vendors often present critical attack vectors in contemporary data breaches. A significant portion of modern breaches involve vendor systems, application

[12] https://www.insurancejournal.com/news/national/2025/05/21/824641.htm (Last accessed Feb. 9, 2026).
[13] https://panorays.com/blog/third-party-risk-management/ (Last accessed Feb. 9, 2026).

programming interfaces, or privileged access maintained by external contractors; inadequate vetting, monitoring, and risk management practices can allow attackers whether external threat actors or compromised insiders to pivot from vendor access to sensitive data systems. [14]

29. Best practices in vendor risk management including continuous monitoring of access, strict background checks, and periodic access rights reviews are widely recognized as essential to prevent unauthorized access and data compromise. Failure to adopt them increases the risk of data loss, theft, and misuse. *Id.*

B. The Data Breach

30. In February 2025, Opexus suffered a catastrophic insider security incident when two engineers, twin brothers Muneeb and Sohaib Akhter, used their authorized access to delete, corrupt, and exfiltrate sensitive data from Opexus systems that stored government agency records.[15]

31. According to investigative reporting, the Akhter brothers were previously convicted of federal cybercrimes, including wire fraud and hacking offenses, yet were nonetheless hired by Opexus to work on its government data

[14] https://auditboard.com/blog/it-vendor-risk-management (Last accessed Feb. 9, 2026).
[15] https://www.insurancejournal.com/news/national/2025/05/21/824641.htm (Last accessed Feb. 9, 2026).

platforms.[16]

32. The breach resulted in the destruction of dozens of databases containing federal agency records, including those related to Freedom of Information Act requests and other stored government information that likely contained sensitive PII submitted by individuals. Independent cybersecurity analyses have termed this an "insider threat attack," highlighting the role that privileged employee access played in enabling the incident.[17]

33. The Akhter brothers' actions disrupted Opexus's core systems (including FOIAXpress and related case management software), leading to data unavailability for government users and potential irretrievable losses of stored records. *Id.*

34. Federal law enforcement agencies, including the FBI, are investigating the incident and have brought charges against the Akhter brothers[18] for unauthorized access, destruction of data, and related computer and identity-theft offenses tied specifically to the data breach at Opexus. [19]

---

[16] https://cyberscoop.com/opexus-background-checks-insider-attack-muneeb-sohaib-akhter/ (Last accessed Feb. 9, 2026).

[17] https://www.adminbyrequest.com/en/blogs/government-data-wiped-by-insider-hackers-in-opexus-security-breach#:~:text=The%20cybersecurity%20world%20got%20a,access%20to%20sensitive%20government%20data. (Last accessed Feb. 9, 2026).

[18] https://hipaatimes.com/twin-brothers-charged-in-federal-contractor-data-breach (Last accessed Feb. 9, 2026).

[19] https://www.bloomberg.com/news/newsletters/2025-12-05/foia-data-breach-leads-to-indictment (Last accessed Feb. 9, 2026).

35. The breach resulted not only in data deletion but also exfiltration of files, meaning that sensitive information, including individual PII, may now reside outside of government and vendor controls in unauthorized hands, creating a realistic risk of misuse. *Id.*

C. Criminal Investigation and Arrests

36. Following the February 2025 data security incident, federal law enforcement authorities initiated a criminal investigation into the unauthorized access, deletion, and exfiltration of government data from Defendant's systems.

37. That investigation was led, in significant part, by federal authorities and the United States Department of Justice investigating the misuse of privileged access to government systems maintained by Defendant.

38. Many of the federal agencies that utilize Defendant's systems are headquartered in Washington, D.C., and rely on those systems to process investigative records, regulatory filings, and Freedom of Information Act requests. The systems affected by the February 2025 insider attack therefore stored and processed information belonging to agencies located in the District of Columbia.

39. Public court records and Department of Justice announcements confirm that the individuals responsible for the insider attack on Defendant's systems were arrested and prosecuted in federal court for offenses arising directly

from their misuse of privileged access to Opexus systems.[20]

40. According to publicly available charging documents, the defendants exploited their positions as trusted insiders to access protected systems, copy sensitive files, and delete critical government databases, conduct that federal prosecutors described as intentional, unauthorized, and criminal. *Id.*

41. Reporting further confirms that the defendants' actions disrupted federal agency operations and compromised systems relied upon by multiple government entities, prompting emergency remediation efforts and coordination with federal law enforcement authorities.[21]

42. The arrests and prosecution of the former employees underscore that the incident was not speculative, accidental, or limited to internal policy violations, but instead constituted criminal conduct involving the misuse of insider access to government data systems.[22]

43. The fact that the criminal investigation, arrests, and prosecution of Defendants working for OPEXUS headquartered in D.C., further demonstrates that Defendant's conduct and failures had substantial connections to this District, including the foreseeable consequences of Defendant's deficient access controls

[20] https://www.justice.gov/opa/pr/two-virginia-men-arrested-conspiring-destroy-government-databases (Last accessed Feb. 9, 2026).
[21] https://www.bloomberg.com/news/newsletters/2025-05-21/how-2-hackers-erased-hundreds-of-foia-requests (Last accessed Feb. 9, 2026).

and monitoring practices.

44. These criminal proceedings also confirm that Defendant's systems lacked adequate safeguards to prevent insiders from engaging in prolonged unauthorized activity without timely detection, despite the availability of well-established industry and government standards designed to prevent exactly this type of misconduct.

D. Defendant Knew or Should Have Known of the Foreseeable Risk of Data Compromise, Theft, and Misuse

45. It is widely recognized in cybersecurity and risk management disciplines that third-party vendor systems handling sensitive data must be subject to robust risk management frameworks to mitigate known threats, including insider misuse and insufficient access controls.[23]

46. Industry standards for vendor risk management require that organizations conduct careful due diligence, verify credentials and background histories for personnel granted elevated access, and implement continuous monitoring to detect anomalous activity before harm occurs.[24]

47. At all relevant times, Opexus entrusted contractor personnel with access to sensitive, non-public government systems, including electronic case-management platforms used to manage audits of government agencies and to

[23] https://auditboard.com/blog/it-vendor-risk-management (Last accessed Feb. 9, 2026).
[24] https://www.xantrion.com/article/cybersecurity-due-diligence-vendor-risk-assessments-a-guide (Last accessed Feb. 9, 2026).

process and track Freedom of Information Act ("FOIA") requests.[25]

48. Such systems necessarily contain sensitive government records and require a heightened duty of care with respect to personnel selection, screening, and access controls.

49. Prior to their employment at Opexus, the two brothers had **previously been prosecuted and sentenced by the United States Government for federal crimes arising from a conspiracy in which they executed a coordinated, multi-stage cyberattack against government systems**, including systems of the United States Department of State, and engaged in wire fraud and other unauthorized access.[26]

50. According to the Department of Justice, that conspiracy involved unauthorized access to sensitive government networks and constituted conduct that "undermined the integrity and security of government information systems." *Id.*

51. The brothers' prior federal criminal convictions allegedly did not appear to be discovered by Opexus at the time of their hiring. According to public reporting, their criminal history only later surfaced when one of the brothers was offered a role with the Federal Deposit Insurance Corporation Office of Inspector

[25] https://www.fedagent.com/news/contractors-background-checks-under-scrutiny-after-massive-breach-traced-to-twin-brothers-previously-convicted-of-hacking (Last accessed Feb. 9, 2026).
[26] https://www.justice.gov/archives/opa/pr/twin-brothers-sentenced-wire-fraud-conspiring-hack-us-department-state-and-private-company (Last accessed Feb. 9, 2026).

General, which required a background check; FDIC officials then learned of the criminal records and flagged the brothers as insider threats, prompting Opexus to take action.[27]

52. This sequence of events is highly concerning. The brothers were not obscure or unknown individuals. Prior to their employment at Opexus, they had been prosecuted and sentenced by the United States Government for federal crimes and their convictions were matters of public record. In addition, they were widely known for their unusually early enrollment at George Mason University, their work on government-funded technology projects, and their subsequent interaction with federal agencies.[28]

53. Given the sensitive nature of the systems to which Opexus granted them access, and the readily discoverable public record of their criminal history and government involvement, Opexus knew or should have known of the brothers' prior convictions through reasonable pre-employment screening and due diligence consistent with federal contractor standards and industry norms.

54. Notwithstanding the sensitive nature of the systems at issue and the foreseeable risk posed by granting internal access to individuals with documented

[27] https://www.bloomberg.com/news/newsletters/2025-12-05/foia-data-breach-leads-to-indictment (Last accessed Feb. 9, 2026).
[28] https://www.washingtonpost.com/local/crime/officials-say-advanced-hack-was-hoax-in-charging-twin-brothers/2015/04/01/17a30c7c-d899-11e4-ba28-f2a685dc7f89_story.html (Last accessed Feb. 9, 2026).

histories of unauthorized access and computer misuse, Opexus failed to implement reasonable hiring, vetting, and supervision safeguards consistent with federal contractor standards and industry norms.

55. As a result, Opexus placed individuals with known criminal histories in positions of trust with access to critical government data systems, directly enabling the data breach and resulting harms.

56. To add to the missteps in hiring, even after the brothers' prior federal criminal convictions were identified and communicated to Opexus, Opexus failed to promptly revoke or restrict their access to sensitive government systems. This failure to immediately suspend or terminate access following notice of the risk violated basic access-control principles and further breached Opexus' duty to safeguard sensitive government data.[29]

57. Cybersecurity accountability frameworks consistently emphasize that organizations must assess risks arising not only from external attackers but also from insiders, especially those with privileges to secure networks and databases.[30]

58. An absence of continuous authentication, least-privilege enforcement, and real-time anomaly detection greatly increases the likelihood of unauthorized

[29] https://cyberscoop.com/opexus-background-checks-insider-attack-muneeb-sohaib-akhter/ (Last accessed Feb. 9, 2026).
[30] https://www.mdpi.com/2079-9292/9/9/1460 (Last accessed Feb. 9, 2026).

data access and theft.[31]

59. Defendant's failures to adhere to known risk-management protocols including lack of real-time monitoring, inadequate background screening, and insufficient restriction of privileged accounts were objectively unreasonable given the foreseeable and documented hazards posed by third-party vendor breaches. *Id.*

E. Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII

60. In the ordinary course of its contracts with government entities, Defendant acquires, collects, receives, and stores highly sensitive electronic data submitted by individuals or contained within agency records, including names, addresses, Social Security numbers, dates of birth, financial account numbers, tax information, driver's license numbers, and other personal identifying details (collectively "PII").

61. The PII that Defendant acquired and stored came from numerous federal, state, and local government sources through client engagements involving FOIA responses, compliance audits, litigation discovery, administrative investigations, and case file management. This PII reflects multiple categories of protected information that the public would expect to remain secure and confidential.

[31] https://www.eccu.edu/blog/third-party-vendor-cyberattacks-and-risk-management (Last accessed Feb. 9, 2026).

62. PII stored on Defendant's systems included information that was *not public at the time of collection*, was submitted by individuals directly for government recordkeeping purposes, and/or otherwise would not be publicly accessible absent Defendant's data processing role.

63. Defendant implicitly and explicitly held itself out as a secure custodian of such sensitive information, representing to agency clients that it would protect the confidentiality, integrity, and availability of data entrusted to its care.

64. Plaintiff and Class Members provided their sensitive PII directly to government agencies or had their PII embedded in records that Defendant acquired, collected, received, transmitted, and stored as part of its role as an outsourced technology provider.

65. Plaintiff first received notice of this breach on January 9, 2026 via written notice from the EEOC.

From: EEOC Data Security <eeoc.data-security@eeoc.gov>
Date: January 9, 2026 at 4:47:24 AM CST

Subject: Notice of Data Security Incident
Reply-To: EEOC Data Security <eeoc.data-security@eeoc.gov>

This notice is to inform you of a data security incident involving information maintained by the U.S. Equal Employment Opportunity Commission (EEOC).

What Happened
The EEOC was recently notified of a data security incident in our Public Portal system, managed by a third-party vendor (Company). Staff employed by the Company, with privileged access to systems, were able to handle data in an unauthorized (UA) and prohibited manner in early 2025. The EEOC was made aware of compromised data around Thursday, December 18, 2025. Upon discovery, the EEOC took immediate steps to secure its systems and initiated an assessment to determine the nature and scope of the incident.

What Information Was Involved
The review determined that certain personally identifiable information (PII) may have been exposed. Depending on the individual, this information may have included name and other identifying or contact information. The review is ongoing, and the EEOC is working with law enforcement.

What We Are Doing
The EEOC takes its responsibility to safeguard information seriously. Shortly after receiving this notice, your Public Portal account password will be reset. The next time you log in to your EEOC account, you will be prompted to reset your password to a stronger, more secure one.
It is also recommended to update your security questions to further safeguard your privacy. Additionally, when you attempt to log in next time, you will be guided through a process that includes signing up for two-factor authentication, adding an extra layer of security by requiring a second form of verification. This is an important security measure designed to protect your account and personal information against unauthorized access and potential security threats.
The EEOC continues to work with the Company and relevant authorities to determine whether any potentially compromised Public Portal accounts have been accessed. If so, information about

additional safeguards will be provided to those directly affected.

What You Can Do
We recommend monitoring financial accounts and credit reports for suspicious activity and remaining alert to potential phishing attempts. The EEOC will not request sensitive information by email or by phone. One precautionary action you can take is to place a 90-day "initial fraud alert" on your credit file. A fraud alert lets creditors know to contact you before opening new accounts, approving loans, or making changes to any existing credit sources.

To place a 90-day "initial fraud alert" on your credit files, call the three nationwide credit reporting companies at the phone numbers listed below or by visiting the links provided.

- **Experian:** 1-888-397-3742 | www.experian.com/fraud/center

- **Equifax:** 1-800-525-6285 | www.equifax.com/personal/credit-report-services/
- **TransUnion:** 1-800-680-7289 | www.transunion.com/fraud-alerts

Additionally, the Consumer Financial Protection Bureau offers a free annual credit report through the following authorized website: www.AnnualCreditReport.com

How You Will Be Updated
The EEOC will communicate any necessary status changes and updates through this same email address (eeoc.data-security@eeoc.gov)

Any questions related to this Public Portal data security incident, you may reply to **eeoc.data-security@eeoc.gov** or call the designated Public Portal data security incident number at **1-888-330-0659.**

Thank you for your attention to this matter. Further updates will be shared as appropriate.

F. The Value of PII

66. Personal identifying information (PII) has significant financial value on illicit markets. Black markets and criminal enterprises trade PII for the purpose

of identity theft, targeted phishing, synthetic identity fraud, credit account takeover, unemployment insurance fraud, and numerous other forms of economic exploitation.

67. The value of an individual's PII, including Social Security numbers, dates of birth, and financial account numbers, is recognized by cybersecurity professionals as substantial because it enables fraudsters to commit identity fraud, assume financial identities, open new credit accounts, receive government benefits, and access existing financial accounts.

68. Research by data security firms and fraud analysts demonstrates that a single complete set of PII can be worth dozens or hundreds of dollars on illegal markets. Even partial records that include combinations of names, addresses, and birthdates have identifiable resale value.

69. Stolen PII is commonly used in fraud schemes that cause victims direct economic harm, including unauthorized credit applications, drain of financial accounts, tax identity theft refund fraud, and other harms requiring years of remediation.

70. Research shows that full identity packets (SSN, DOB, etc.) can sell on dark web markets for significant sums, reflecting high demand.[32]

71. FTC and cybersecurity firms emphasize the enduring value of PII to

[32] https://deepstrike.io/blog/dark-web-data-pricing-2025 (Last accessed Feb. 9, 2026).

malicious actors and the long-term risk it poses to affected individuals.

G. Defendant Failed to Comply with Industry Standards

72. Reasonable data security for entities entrusted with sensitive personal information requires implementing controls commensurate with the sensitivity of the data and the foreseeability of internal and external threats, including insider misuse. Federal guidance and widely adopted cybersecurity frameworks emphasize least-privilege access, strong auditing/logging, privileged-user monitoring, and rapid deprovisioning of access upon termination or role change. [33]

73. The National Institute of Standards and Technology ("NIST") has published baseline security and privacy controls, most notably in NIST Special Publication 800-53 Revision 5 that expressly address privileged access governance, audit logging, and access control, controls that are widely treated as minimum expectations for organizations handling sensitive information, including federal contractor environments. *Id.*

74. Among those baseline expectations is the principle of least privilege which mandates that organizations limit user and process permissions to the minimum necessary to perform assigned functions, with heightened restrictions

[33] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (Last accessed Feb. 9, 2026).

for administrative and privileged users. NIST SP 800-53 Rev. 5 specifically requires enforcement of least privilege, separation of duties, and periodic review of privileged accounts to reduce the risk of abuse or misuse. *Id.* [34]

75. Industry best practices likewise require robust insider-threat mitigation, including (i) continuous monitoring and alerting for anomalous behavior by privileged users; (ii) controls to prevent or detect bulk copying or mass export of sensitive files; (iii) data loss prevention ("DLP") mechanisms to restrict transfers to removable media or unauthorized destinations; and (iv) strong offboarding procedures to immediately revoke access at or before termination. [35]

76. NIST further requires organizations to implement audit logging and monitoring controls sufficient to detect and investigate inappropriate or anomalous activity by privileged users, including actions affecting large volumes of data or critical system components. These controls include centralized logging, retention of audit records, and automated analysis to identify suspicious behavior indicative of insider threats. *Id.*

77. Here, public reporting and governmental materials describe an incident in which individuals with privileged access were able to delete numerous government databases and copy large volumes of agency files, underscoring the

[34] https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-6/ (Last accessed Feb. 9, 2026).
[35] https://www.cisa.gov/sites/default/files/2022-11/Insider%20Threat%20Mitigation%20Guide_Final_508.pdf (Last accessed Feb. 9, 2026).

absence of effective least-privilege restrictions, monitoring, and offboarding controls that would be expected under reasonable, industry-standard security practices. [36]

78. Public reporting further reflects that Defendant characterized the incident as an insider threat and that investigations highlighted significant security failures, facts that are consistent with the conclusion that Defendant's controls fell below accepted standards for a contractor handling sensitive government and third-party information. [37]

79. Defendant's deviations from accepted industry standards were especially unreasonable because the relevant risks, insider misuse, privileged account abuse, and retaliation during termination/offboarding, are well-documented and specifically addressed by authoritative guidance and best-practice frameworks.

H. Defendant Failed to Comply with FTC Guidelines

80. The Federal Trade Commission ("FTC") has established guidelines instructing companies that collect and maintain sensitive consumer information to implement reasonable and appropriate safeguards to protect that information from

[36] https://cyberscoop.com/opexus-background-checks-insider-attack-muneeb-sohaib-akhter/ (Last accessed Feb. 9, 2026).
[37] https://www.bloomberg.com/news/articles/2025-05-21/security-failures-behind-us-contractor-s-data-breach (Last accessed Feb. 9, 2026).

unauthorized access, disclosure, misuse, and breach.

81. According to the FTC's framework, entities that store PII should adopt comprehensive information security programs that include (a) risk assessment, (b) access controls, (c) background screening, (d) monitoring for unauthorized activity, (e) encryption of sensitive data at rest and in transit, and (f) employee training on cybersecurity risks.

82. The FTC's own published guidance further confirms this framework. In its February 2025 Privacy Impact Assessment for the FOIAXpress system, the OPEXUS platform used to store and process sensitive nonpublic records containing PII, the FTC explained that such safeguards are necessary to mitigate the risk of insider misuse and unauthorized access. It states, "Opexus maintains its own incident response plan, which outlines procedures for reporting information security incidents, including communications, restoring services, and providing breach notifications. The FTC's contract with Opexus requires the company to immediately notify the agency of any breaches that may affect FTC data."[38]

83. The FTC has repeatedly taken enforcement actions against companies whose failure to comply with these principles resulted in data breaches that harmed consumers, demonstrating that such safeguards are required and that inadequate

[38] https://www.ftc.gov/system/files/ftc_gov/pdf/february-2025-foiaxpress-pia.pdf (Pg. 7). (Last accessed Feb. 9, 2026).

protections constitute unfair or deceptive practices.

84. Defendant's failure to implement reasonable access restrictions, background vetting, continuous monitoring, least-privilege enforcement, and robust authentication mechanisms violated these well-established FTC data security guidelines.

85. Defendant's deficient security resulted in the unauthorized deletion, exfiltration, and potential compromise of PII, and thus violated the expectations that federal guidelines, including those published by the FTC, provide to companies entrusted with sensitive data.

86. FTC guidance on data security measures, including access controls and monitoring, further emphasizes industry standards and enforcement history.[39]

I. Plaintiff and Class Members Suffered Damages

87. As a direct and proximate result of Defendant's failures, Plaintiff and putative Class Members suffered the compromise and loss of control of their private information; the unauthorized exposure, access, copying, deletion, and/or destruction of data; and the resulting increased risk of identity theft and fraud.

88. Identity theft and fraud are well-recognized consequences of the exposure of sensitive identifiers. The Federal Trade Commission advises

[39] https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business (Last accessed Feb. 9, 2026).

consumers that identity thieves can use exposed information to engage in unauthorized transactions and other forms of financial misuse, and that vigilance and protective steps are necessary where data exposure is suspected. [40]

89. Data-breach victims reasonably incur out-of-pocket costs and time losses to prevent, detect, and remediate fraud, including costs for credit monitoring, credit freezes, fraud alerts, account changes, additional security measures, and ongoing monitoring of financial and other accounts. [41]

90. These mitigation efforts are time-consuming and can extend for long periods. Government statistical reporting reflects that, among victims whose personal information is used fraudulently, a substantial portion spend a month or more resolving resulting problems.

91. Beyond direct out-of-pocket losses and time burdens, Plaintiff and Class Members also suffered the loss of privacy and the loss of the benefit of reasonable data security practices promised or implied by Defendant's role as a trusted custodian of sensitive data.

92. The harms resulting from data compromise are long-lasting because sensitive identifiers, once disclosed, cannot be "recalled," and remain valuable for misuse over time. Public reporting and consumer-protection guidance consistently

[40] https://consumer.ftc.gov/consumer-alerts/2022/02/how-tell-if-someone-using-your-identity (Last accessed Feb. 9, 2026).
[41] https://consumer.ftc.gov/articles/credit-freezes-and-fraud-alerts (Last accessed Feb. 9, 2026).

emphasize that exposed information can be leveraged repeatedly for fraud, making continuing monitoring and protective actions reasonably necessary.

93. Separately and independently, Plaintiff and putative Class Members suffered injury from Defendant's failure to maintain reasonable safeguards, including the heightened risk of future misuse so long as Defendant retains personal information without demonstrating that it has implemented and maintained adequate security controls consistent with industry standards. [42]

J. Defendant's Delay in Identifying and Reporting the Data Breach Caused Additional Harm

94. Timely breach detection and notification are essential because they allow affected individuals to take prompt steps to limit fraud, reduce damages, and protect their financial and personal security. Consumer-protection guidance emphasizes that learning of a breach quickly enables consumers to monitor accounts, change credentials, and place credit freezes or fraud alerts, actions that can reduce the likelihood and impact of identity theft. [43]

95. The practical importance of rapid protective action is reflected in federal guidance describing concrete steps individuals should take when they

[42] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf (Last accessed Feb. 9, 2026).
[43] https://www.consumerreports.org/electronics/data-theft/the-data-breach-next-door-a7102554918 (Last accessed Feb. 9, 2026).

suspect identity misuse, including monitoring statements and setting alerts, steps that depend on timely knowledge that sensitive information may have been exposed. [44]

96. Public reporting and governmental materials describe a February 2025 incident involving privileged insiders' unauthorized activities affecting government databases and files, with subsequent criminal investigation and charging decisions reflecting the seriousness of the incident and the risks it created. *Id.*

97. Upon information and belief, Defendant and/or impacted agencies learned of the incident near the time it occurred, given the operational disruption, investigative response, and law-enforcement involvement described in public reporting; yet many affected individuals did not receive timely, actionable notice that would have allowed them to undertake protective measures at the earliest possible moment. [45]

98. This delay deprived Plaintiff and putative Class Members of the opportunity to take prompt mitigation steps, increasing their risk of fraud and extending the period in which criminals could misuse exposed information without victims' awareness.

[44] https://www.identitytheft.gov/Steps (Last accessed Feb. 9, 2026).
[45] https://www.bloomberg.com/news/articles/2025-05-21/security-failures-behind-us-contractor-s-data-breach (Last accessed Feb. 9, 2026).

99. The delay also foreseeably increased Plaintiff's and putative Class Members' time and monetary costs because the longer a breach remains undisclosed, the longer consumers go without implementing protective measures (e.g., freezes, alerts, enhanced monitoring) that can help prevent or limit fraud-related damages.

100. Defendant's failure to provide timely, meaningful notice and actionable detail further compounded harm by forcing Plaintiff and putative Class Members to mitigate in the dark, without adequate information regarding what data categories were implicated, what systems were affected, and what protective measures were most appropriate under the circumstances.

V. CLASS ACTION ALLEGATIONS

A. Class Definitions

101. Plaintiff brings this action pursuant to Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure on behalf of himself and all others similarly situated.

102. Plaintiff seeks to represent the following Nationwide Class, defined as:

> All persons in the United States whose Personal Identifying Information ("PII") was accessed, copied, exfiltrated, destroyed, compromised, or placed at a material risk of misuse as a result of the February 2025 Opexus data breach.

103. Plaintiff also seeks to represent the following Alabama Subclass, defined as:

> All persons residing in the State of Alabama whose PII was accessed, copied, exfiltrated, destroyed, compromised, or placed at a material risk of misuse as a result of the February 2025 Opexus data breach.

104. Excluded from the Classes are Defendant, its officers, directors, members, employees, affiliates, parents, subsidiaries, legal representatives, successors, assigns, and any judicial officer presiding over this matter and their immediate family members.

105. Plaintiff reserves the right to amend or modify the class definitions as discovery reveals additional facts, including the creation of additional subclasses as appropriate.

B. Numerosity

106. The Classes are so numerous that joinder of all members is impracticable. Defendant provides data management services to numerous government agencies nationwide, and the breach impacted systems containing records relating to thousands, if not tens of thousands, of individuals.

107. The exact number of Class Members is known to Defendant and can be readily ascertained through Defendant's records, audit logs, client notifications, and breach-response documentation.

C. Commonality

108. This action presents questions of law and fact common to all Class Members, including but not limited to:

a. Whether Defendant owed Plaintiff and Class Members a duty to safeguard their PII;

b. Whether Defendant failed to implement reasonable data security measures;

c. Whether Defendant failed to comply with industry standards and regulatory guidance;

d. Whether Defendant failed to timely detect, prevent, and remediate the breach;

e. Whether Defendant failed to provide timely and adequate notice of the breach;

f. Whether Plaintiff's and Class Members' PII was accessed, copied, exfiltrated, deleted, or otherwise compromised;

g. Whether Defendant's conduct caused Plaintiff and Class Members to suffer damages;

h. Whether Defendant's conduct violated state consumer protection statutes, including the Alabama Deceptive Trade Practices Act;

i. Whether Defendant's conduct warrants injunctive and equitable relief.

109. These common questions arise from Defendant's uniform course of conduct and are capable of class-wide resolution.

D. Typicality

110. Plaintiff's claims are typical of the claims of the Class Members because Plaintiff and all Class Members were subjected to the same data security failures, the same breach event, and the same deficient detection and notification

practices.

111. Plaintiff's injuries arise from the same operative facts and legal theories as those of the Class Members, including negligence, statutory violations, loss of privacy, mitigation costs, and increased risk of future harm.

112. Plaintiff does not assert any claims that are antagonistic to or in conflict with the interests of the Classes.

E. Adequacy of Representation

113. Plaintiff will fairly and adequately protect the interests of the Classes.

114. Plaintiff has no interests adverse to those of the Class Members and has retained counsel experienced in complex class action litigation, data breach cases, and consumer protection matters.

115. Plaintiff and Class Counsel are committed to prosecuting this action vigorously on behalf of the Classes.

F. Predominance and Superiority (Rule 23(b)(3))

116. Common questions of law and fact predominate over any questions affecting only individual members of the Classes. Defendant's liability arises from standardized, centralized conduct, namely, its uniform failure to implement reasonable cybersecurity controls, prevent insider misuse, and timely notify affected individuals.

117. Issues of causation, breach, and damages can be established through

common proof, including Defendant's own records, forensic findings, incident response materials, and uniform security policies.

118. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because:

a. Individual litigation would be impracticable and inefficient;

b. The damages suffered by individual Class Members are substantial but may be insufficient to justify individual actions;

c. Class treatment promotes consistency of adjudication and judicial economy;

d. Defendant's conduct is best addressed through a single coordinated proceeding.

G. Injunctive and Declaratory Relief (Rule 23(b)(2))

119. Defendant has acted or refused to act on grounds generally applicable to the Classes by failing to implement and maintain reasonable data security practices.

120. Plaintiff seeks injunctive and declaratory relief requiring Defendant to:

a. Enforce least-privilege access and insider-threat mitigation controls;

b. Conduct regular security audits and risk assessments;

c. Provide ongoing protections for Class Members whose data remains at risk; and

d. Implement industry-standard cybersecurity safeguards.

121. Such relief is appropriate for the Classes as a whole because Defendant's deficient practices continue to pose a material risk of future harm.

CAUSES OF ACTION

COUNT I
Negligence and Negligence Per Se
(On Behalf of Plaintiff and the Nationwide Class)

122. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

123. Defendant owed Plaintiff and Class Members a duty to exercise reasonable care in the collection, storage, maintenance, transmission, and protection of Plaintiff's and Class Members' PII.

124. This duty arose from multiple, independent sources, including but not limited to:

a. Defendant's role as a federal government contractor and professional data custodian entrusted with sensitive personal and government-related information;

b. Defendant's role as a professional data custodian entrusted with sensitive personal and government-related information;

c. Defendant's affirmative representations and implied assurances that it would safeguard data using reasonable security measures;

d. Defendant's superior knowledge, access, and control over the systems storing Plaintiff's and Class Members' PII; and

e. The foreseeable risk of harm resulting from unauthorized access, insider misuse, exfiltration, or destruction of such information.

125. Defendant further owed a duty to implement and maintain reasonable

administrative, technical, and physical safeguards appropriate to the sensitivity of the data it handled, including safeguards to prevent, detect, and respond to insider threats.

126. Defendant also owed Plaintiff and Class Members a duty to timely identify, investigate, and disclose security incidents involving their PII so that affected individuals could take reasonable steps to mitigate harm.

127. Defendant breached its duties by failing to exercise reasonable care in safeguarding Plaintiff's and Class Members' PII.

128. Defendant's breaches include, but are not limited to, the following acts and omissions:

a. Failing to implement and enforce least-privilege access controls for personnel with access to sensitive systems;

b. Granting and maintaining privileged system access for individuals without adequate vetting, supervision, and monitoring;

c. Failing to implement effective controls to prevent or detect bulk copying, deletion, or exfiltration of sensitive files;

d. Failing to implement adequate insider-threat monitoring, logging, and alerting mechanisms;

e. Failing to promptly revoke or restrict system access during termination or role changes;

f. Failing to timely detect the unauthorized activity that resulted in the breach;

g. Failing to timely notify Plaintiff and Class Members of the breach and its scope.

h. Failing to implement and enforce cybersecurity safeguards consistent with standards applicable to federal contractors handling sensitive government information.

129. Defendant's conduct fell well below the standard of care expected of a reasonable entity entrusted with sensitive personal information, particularly one operating as a government contractor handling regulated and confidential data.

130. Defendant's conduct also constitutes negligence per se because it violated duties imposed by federal statutes, regulatory guidance, and authoritative cybersecurity standards designed to protect individuals from unauthorized access, disclosure, and misuse of sensitive personal information.

131. The Federal Trade Commission has repeatedly articulated that failure to implement reasonable data security measures constitutes an unfair practice under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. FTC guidance, enforcement actions, and consent orders establish baseline requirements for reasonable data security, including risk assessment, access controls, monitoring, and incident response.

132. Defendant violated these duties by failing to implement reasonable safeguards to protect Plaintiff's and Class Members' PII, thereby engaging in conduct that the FTC has repeatedly identified as unfair and unreasonable.

133. In addition, widely accepted cybersecurity standards promulgated by the National Institute of Standards and Technology ("NIST"), including NIST Special Publication 800-53, identify minimum security controls for organizations handling sensitive information.

134. Defendant's failure to implement and maintain controls consistent with these standards constitutes a deviation from the standard of care and further supports negligence per se.

135. Plaintiff and Class Members are within the class of persons these statutes, regulations, and standards were intended to protect, and the harms suffered, including loss of privacy, increased risk of identity theft, mitigation costs, and data misuse, are the types of harms these authorities were designed to prevent.

136. Defendant's negligent acts and omissions were the direct and proximate cause of Plaintiff's and Class Members' injuries.

137. But for Defendant's failure to implement reasonable security measures, insider-threat controls, and monitoring safeguards, Plaintiff's and Class Members' PII would not have been accessed, copied, exfiltrated, destroyed, or placed at a material risk of misuse.

138. Defendant's failure to timely detect and disclose the breach further caused Plaintiff and Class Members to suffer additional harm by depriving them of the opportunity to promptly mitigate the risk of identity theft and fraud.

139. As a direct and proximate result of Defendant's negligence and negligence per se, Plaintiff and Class Members have suffered damages, including but not limited to: Loss of privacy and control over their PII, out-of-pocket expenses incurred to mitigate the risk of identity theft and fraud; time and productivity losses

associated with monitoring accounts, placing fraud alerts or credit freezes, and addressing security concerns; increased risk of future identity theft and fraud; emotional distress and anxiety resulting from the exposure of sensitive personal information.

140. Plaintiff and Class Members also face a continuing risk of harm so long as Defendant retains their PII without demonstrating that it has implemented adequate, industry-standard security measures.

141. Plaintiff and Class Members seek all available relief under applicable federal and state law, including compensatory damages, statutory damages where available, injunctive relief requiring Defendant to implement reasonable and industry-standard cybersecurity safeguards, costs, attorneys' fees, and such other relief as the Court deems just and proper.

COUNT II
Negligent and Wanton Hiring, Retention, and Supervision
(On Behalf of Plaintiff and the Nationwide Class)

142. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

143. Defendant owed Plaintiff and Class Members a duty to exercise reasonable care in the hiring, retention, supervision, and access authorization of employees and contractor personnel entrusted with access to sensitive government systems and Plaintiff's and Class Members' personally identifiable information

("PII").

144. This duty arose from, among other things:

a. Defendant's role as a federal government contractor and data custodian entrusted with sensitive, non-public government and personal information maintained on behalf of federal agencies;

b. Defendant's role as a federal contractor and data custodian entrusted with sensitive, non-public government and personal information;

c. The foreseeable risk of harm posed by insider misuse, privileged account abuse, and retaliatory conduct by individuals granted elevated system access;

d. Defendant's exclusive control over personnel screening, access provisioning, monitoring, and offboarding decisions; and

e. Widely recognized industry standards and federal guidance requiring reasonable vetting, supervision, and access governance for personnel with access to sensitive systems.

145. Prior to their employment with Defendant, individuals later responsible for the intrusion, destruction, and copying of government data had been prosecuted and sentenced by the United States Government for federal crimes involving unauthorized access to government computer systems and related misconduct. These convictions were matters of public record at the time Defendant hired and granted those individuals privileged system access.

146. Defendant's failure to act upon notice of a known and foreseeable insider threat constituted a breach of its duties of reasonable hiring, retention, and supervision, and reflected a conscious disregard for the safety and security of Plaintiff's and Class Members' information.

147. Defendant's acts and omissions were negligent, reckless, and wanton in that Defendant knew or should have known that granting and maintaining privileged access to individuals with known histories of unauthorized system access created a substantial and unreasonable risk of harm, yet failed to take reasonable steps to prevent that harm.

148. As a direct and proximate result of Defendant's negligent and wanton hiring, retention, and supervision, individuals with privileged access were able to delete government databases, copy large volumes of sensitive agency files, and compromise Plaintiff's and Class Members' PII.

149. The harms suffered by Plaintiff and Class Members, including loss of privacy, loss of control over personal information, increased risk of identity theft and fraud, mitigation costs, and emotional distress, were foreseeable consequences of Defendant's failure to reasonably screen, supervise, and restrict access by its personnel.

150. Defendant's negligent and wanton conduct was a substantial factor in causing Plaintiff's and Class Members' injuries and occurred independently of, and in addition to, Defendant's failures to implement reasonable technical security safeguards as alleged in Count I.

151. As a result of Defendant's negligent and wanton hiring, retention, and supervision, Plaintiff and Class Members are entitled to all available relief under

applicable law, including compensatory damages, punitive or exemplary damages where permitted, injunctive relief requiring Defendant to implement reasonable personnel-security and insider-threat safeguards, costs, attorneys' fees, and such other relief as the Court deems just and proper.

COUNT III
INVASION OF PRIVACY
(On Behalf of Plaintiff and the Nationwide Class)

152. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

153. Plaintiff and Class Members had a reasonable and legitimate expectation of privacy in their Personal Identifying Information ("PII"), including but not limited to names, Social Security numbers, dates of birth, addresses, financial identifiers, and other sensitive personal data.

154. Plaintiff and Class Members entrusted their PII to federal government entities for limited and specific purposes, with the reasonable expectation that such information would be protected from unauthorized access, disclosure, copying, misuse, or destruction.

155. Defendant, as a third-party data custodian and government contractor, assumed a duty to preserve the confidentiality and privacy of Plaintiff's and Class Members' PII and to restrict access to that information to authorized persons acting for legitimate purposes only.

156. Defendant, through its reckless disregard for the privacy rights of Plaintiff and Class Members, failed to implement and maintain reasonable safeguards to prevent unauthorized access to, and misuse of, Plaintiff's and Class Members' PII.

157. As a direct result of Defendant's conduct, Plaintiff's and Class Members' PII was accessed, copied, exfiltrated, deleted, destroyed, and/or otherwise compromised by unauthorized individuals, including insiders who lacked any legitimate purpose for such access.

158. The unauthorized access to and compromise of Plaintiff's and Class Members' PII constitutes an intrusion into their private affairs that would be highly offensive to a reasonable person.

159. Defendant's failures enabled the exposure of sensitive personal information in a manner that violated Plaintiff's and Class Members' right to privacy, including the right to control access to and dissemination of their personal information.

160. Defendant knew or should have known that its deficient cybersecurity practices and failure to mitigate insider threats created a substantial risk that Plaintiff's and Class Members' PII would be improperly accessed and misused.

161. Defendant's conduct constitutes an invasion of privacy under applicable common law principles because it resulted in the unauthorized intrusion

upon Plaintiff's and Class Members' seclusion and private affairs, and/or the unauthorized disclosure of private facts concerning Plaintiff and Class Members.

162. As a direct and proximate result of Defendant's invasion of privacy, Plaintiff and Class Members suffered injuries.

163. Defendant's conduct was willful, wanton, reckless, and/or demonstrated a conscious disregard for the privacy rights of Plaintiff and Class Members.

164. Plaintiff and Class Members have no adequate remedy at law to fully address the ongoing invasion of their privacy, because Defendant continues to retain their PII without demonstrating that it has implemented adequate safeguards to prevent further unauthorized access or misuse.

165. Unless enjoined and restrained by this Court, Defendant's wrongful conduct will continue to place Plaintiff's and Class Members' private information at risk of further invasion and misuse.

166. Plaintiff and Class Members seek all relief available under law for Defendant's invasion of privacy, including compensatory damages, injunctive and equitable relief, costs, attorneys' fees, and such other relief as the Court deems just and proper.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Nationwide Class)

167. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

168. . Defendant occupied a position of trust and confidence with respect to Plaintiff and Class Members by virtue of its role as a third-party data custodian and federal government contractor entrusted with sensitive personal information collected and stored on behalf of federal agencies.

169. Plaintiff and Class Members were required to provide, or had embedded within agency records, highly sensitive PII for limited and specific purposes, and they reasonably relied on Defendant to safeguard that information and to prevent unauthorized access, disclosure, misuse, or destruction.

170. Defendant possessed superior knowledge, expertise, and exclusive control over the systems, networks, and security practices governing Plaintiff's and Class Members' PII, while Plaintiff and Class Members lacked any meaningful ability to monitor, access, or protect that information once entrusted to Defendant.

171. By voluntarily undertaking the responsibility of collecting, storing, managing, and securing Plaintiff's and Class Members' PII, Defendant assumed fiduciary and/or confidential obligations to act in the best interests of Plaintiff and Class Members with respect to that information.

172. Defendant further reinforced this relationship of trust by representing expressly and impliedly, that it maintained reasonable and industry-standard security measures and that it could be trusted to protect sensitive data from unauthorized access and misuse.

173. Defendant breached its fiduciary duties of care, loyalty, and confidentiality owed to Plaintiff and Class Members by, among other things:

a. Granting and maintaining excessive or inadequately supervised system access to individuals with privileged roles;

b. Failing to detect, prevent, or timely respond to insider misuse of its systems;

c. Failing to promptly revoke access during termination or role changes;

d. Failing to timely notify Plaintiff and Class Members of the data breach and its scope; and

e. Failing to take reasonable steps to mitigate harm after the breach occurred.

f. Failing to implement and enforce safeguards consistent with standards applicable to federal contractors entrusted with sensitive government information.

174. Defendant's conduct placed its own operational convenience, cost savings, and internal practices above the privacy and security interests of Plaintiff and Class Members, in direct contravention of its fiduciary obligations.

175. Defendant knew or should have known that its failures created a substantial and foreseeable risk of harm to Plaintiff and Class Members, including loss of privacy, identity theft, and fraud.

176. Defendant's breaches of fiduciary duty were the direct and proximate cause of Plaintiff's and Class Members' injuries.

177. As a result of Defendant's misconduct, Plaintiff and Class Members suffered damages.

178. Defendant's breaches also deprived Plaintiff and Class Members of the benefit of the confidential relationship and trust they were entitled to expect when their data was entrusted to Defendant's care.

179. Plaintiff and Class Members have no adequate remedy at law to fully redress Defendant's breaches because Defendant continues to retain their PII and continues to expose them to a risk of further harm absent judicial intervention.

180. Defendant's conduct was willful, wanton, reckless, and/or in conscious disregard of its fiduciary duties, entitling Plaintiff and Class Members to all available legal and equitable relief.

COUNT V
VIOLATION OF THE ALABAMA DECEPTIVE TRADE PRACTICES ACT
Ala. Code §§ 8-19-1 et seq.
(On Behalf of Plaintiff and the Alabama Subclass)

181. Plaintiff realleges and incorporates by reference all preceding allegations as though fully set forth herein.

182. The Alabama Deceptive Trade Practices Act ("ADTPA"), Ala. Code §§ 8-19-1 et seq., prohibits unfair, false, misleading, and deceptive acts or practices

in the conduct of trade or commerce.

183. Defendant is a "person" and "supplier" within the meaning of the ADTPA because it engaged in trade or commerce by providing data management and technology services in the ordinary course of its business that involved the collection, storage, processing, and retention of personal information belonging to Alabama residents.

184. Plaintiff and members of the Alabama Subclass are "consumers" within the meaning of the ADTPA because they are natural persons whose personal information was collected, stored, processed, and retained in connection with Defendant's services.

185. Defendant's conduct occurred in or affected trade or commerce because Defendant's representations, omissions, and practices concerning data security and breach disclosure directly impacted Alabama residents whose personal information Defendant maintained.

186. Defendant engaged in unlawful deceptive acts and practices in violation of Ala. Code § 8-19-5 by representing, expressly and impliedly, that it implemented reasonable and appropriate data security measures to safeguard sensitive personal information, when in fact it did not.

187. Defendant's deceptive acts include, but are not limited to:

188. Representing that its services were of a particular standard, quality, or

grade with respect to data security when they were not.

189. Defendant's omissions and misrepresentations were material because reasonable consumers would consider information concerning the security of their personal data, and whether it had been compromised, important in deciding what steps to take to protect themselves from identity theft, fraud, and other harms.

190. Defendant's conduct created a likelihood of confusion or misunderstanding among Plaintiff and Alabama Subclass Members regarding the safety and security of their personal information, in violation of Ala. Code § 8-19-5(1), (5), (7), and (27).

191. As a direct and proximate result of Defendant's deceptive acts and practices, Plaintiff and Alabama Subclass Members suffered ascertainable losses, including but not limited to:

a. Out-of-pocket expenses incurred to monitor and protect against identity theft and fraud;

b. Time and effort expended to mitigate the risk of misuse of their personal information;

c. Loss of the benefit of the bargain for reasonable data security practices; and

d. Loss of privacy and control over their personal information.

192. Defendant's deceptive conduct also subjected Plaintiff and Alabama Subclass Members to a continuing and unreasonable risk of identity theft and fraud, constituting an ongoing injury so long as Defendant retains their personal information without demonstrating that it has implemented adequate security

safeguards.

193. Plaintiff and Alabama Subclass Members reasonably relied on Defendant's representations and omissions concerning its data security practices and were injured as a result.

194. Plaintiff seeks injunctive relief on behalf of himself and the Alabama Subclass to enjoin Defendant from continuing its deceptive practices.

195. Pursuant to Ala. Code § 8-19-10(a)(3), Plaintiff seeks reasonable attorneys' fees and costs incurred in bringing this action on behalf of the Alabama Subclass.

196. Defendant's violations of the ADTPA were willful, knowing, and in reckless disregard of the rights of Plaintiff and the Alabama Subclass.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Nationwide Class and Alabama Subclass, respectfully requests that this Court enter judgment against Defendant and grant the following relief:

a. Certifying this action as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure;

b. Appointing Plaintiff as Class Representative for the Nationwide Class and the Alabama Subclass;

c. Appointing Plaintiff's counsel as Class Counsel for the Nationwide

Class and the Alabama Subclass;

d. Awarding Plaintiff and Class Members compensatory damages in an amount to be determined at trial, including damages for loss of privacy, loss of control over personal information, emotional distress, and other actual and consequential damages suffered as a result of Defendant's conduct;

e. Awarding Plaintiff and Class Members statutory damages, treble damages, or enhanced damages as authorized by applicable law;

f. Awarding pre-judgment and post-judgment interest at the maximum rate permitted by law;

g. Enjoining and restraining, temporarily, preliminarily and permanently, Defendant from continuing to engage in the wrongful acts and practices alleged herein and directing Defendant to certify under oath that it has fully complied with any directive from this Court concerning any injunctive relief;

h. Entering appropriate declaratory relief declaring that Defendant's conduct violated applicable common law duties and consumer protection statutes;

i. Awarding Plaintiff and Class Members their reasonable attorneys' fees, litigation expenses, expert fees, and costs as permitted by

applicable law, including under the the Alabama Deceptive Trade Practices Act;

j. Awarding such other and further relief as the Court deems just, proper, and equitable.

JURY DEMAND

Plaintiff requests a trial by jury.

Respectfully submitted this the 16th of March y 2026.

/s/ Nathan M. Peak
Nathan M. Peak
BRACKER & MARCUS LLC
3355 Lenox Rd NE, Ste. 660
Atlanta, GA 30326
Phone: 770-988-5035
Fax: 678-648-5544
Nathan@fcacounsel.com

/s/ *D. Anthony Mastando*
D. Anthony Mastando (ASB-0893-X32B)
Eric J. Artrip (ASB-9673-I68E)
Applying for Pro Hac Vice
MASTANDO & ARTRIP, LLC
301 Holmes Ave., NE, Ste. 100
Huntsville, Alabama 35801
Phone: (256) 532-2222
Fax: (256) 513-7489
tony@mastandoartrip.com
artrip@mastandoartrip.com

/s/ *Nickolas J. Hagman*
Nickolas J. Hagman (Illinois Bar 6317689)
CAFFERTY CLOBES
MERIWETHER & SPRENGEL LLP
Applying for Pro Hac Vice
135 S. LaSalle, Suite 3210
Chicago, Illinois 60603
Telephone: (312) 782-4880
Facsimile: (312) 782-4485
nhagman@caffertyclobes.com

DEFENDANTS TO BE SERVED VIA CERTIFIED MAIL

AINS, LLC d/b/a OPEXUS a/k/a CASEPOINT
1101 17th Street NW, 12th Floor
Washington, D.C. 20036