

**UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA**

TRISTYN EDWARDS and MORGAN
STAMPFLI, on behalf of themselves and all
others similarly situated,

Plaintiffs,

vs.

UNITED STATES DEPARTMENT OF
WAR,
1400 Defense Pentagon,
Washington, D.C. 20301,

Defendant.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CASE NO. _____

CLASS ACTION COMPLAINT

Plaintiffs Tristyn Edwards (“Mr. Edwards”) and Morgan Stampfli (“Mr. Stampfli”) (collectively, “Plaintiffs”), individually and on behalf of the proposed class described below, bring this action for injunctive relief and actual and statutory damages against the United States Department of War (“DOW” or “Defendant”). Facts pertaining to Plaintiffs and their personal experiences and circumstances are alleged based upon personal knowledge, and all other facts herein are alleged based upon information and belief, as well as, *inter alia*, the investigation of Plaintiffs’ counsel.

NATURE OF THE CASE

1. This case arises out of the cyber-breach of the Defense Manpower Data Center (“DMDC”), resulting in the unauthorized disclosure of sensitive personally identifiable

information (“PII” or “Private Information”) of approximately 3.05 million individuals, including social security numbers (“SSNs”) (the “Data Breach”).¹

2. The DMDC operates under the DOW “to collate personnel, manpower, training, financial, and other data” for the Department. “This data catalogues the history of personnel in the military and their family for purposes of healthcare, retirement funding, and other administrative needs.” As of Fiscal Year 2024, DMDC held more than 60 million records pertaining to DOW servicemembers, civilian staff, contractors, family members, retirees, and veterans.² DMDC also oversees identity verification for all DOW ID card holders.³

3. On or around July 16, 2026, Defendant discovered a vulnerability in a DMDC file sharing system, which allowed unauthorized users to access files containing PII of millions of servicemembers and military-adjacent individuals. Unauthorized users were able to access the DMDC file sharing system for nearly *nine months* completely unnoticed, as the unauthorized access activity began in October 2025.⁴ The result of this long-unnoticed breach is the extraction of various pieces of sensitive PII, including SSNs, full names, dates of birth, contact information, sex, race, and military personnel information, including occupational specialty.⁵

¹ See Rachel S. Cohen, *More than 3 million people affected by military data breach*, Federal News Network (Sept. 28, 2026), <https://federalnewsnetwork.com/defense-main/2026/09/more-than-3-million-people-affected-by-military-data-breach> (hereinafter “Cohen Data Breach Article”).

² See DMDC, *DMDC Overview*, DOW, <https://dwp.dmdc.osd.mil/dwp/app/about/overview> (last visited Oct. 20, 2026) (hereinafter “DMDC Overview”).

³ See Cohen Data Breach Article.

⁴ See David DiMolfetta, *Unauthorized users accessed sensitive records for roughly nine months before discovery, exposing another government personnel data fiasco as the FBI confronts its own breach incident.*, NextGov/FCW (Oct. 5, 2026), <https://www.nextgov.com/cybersecurity/2026/10/pentagon-personnel-breach-undetected-months-renews-cyber-standard-scrutiny/416414/?oref=ng-homepage-river>.

⁵ See Sead Fadilpašić, *Massive Pentagon hack sees records of 2.7 million US military personnel leaked during months-long data breach—names, military service records, and*

4. Despite discovering the breach in July, notice of the breach was not sent to impacted individuals until late September or early October 2026. Defendant's failure to promptly notify Plaintiffs and Class members has resulted in these individuals experiencing misuse of their PII. Some, such as Mr. Edwards and Mr. Stampfli, have experienced actual fraud on their accounts and drastic increases in spam calls and emails. The exposure of Plaintiff and Class members' PII will cause various types of misuse in the coming months and years, including but not limited to, unauthorized credit card charges, unauthorized access to email accounts, identity theft, and other fraudulent use of their Private Information.

5. There has been no assurance offered from DMDC that all personal data or copies of data have been recovered or destroyed.

6. Accordingly, Plaintiffs assert claims based on violation of the Privacy Act of 1974 on behalf of themselves and all others similarly situated.

JURISDICTION AND VENUE

7. This Court has subject matter jurisdiction over all claims in this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because: "the parties are minimally diverse, the class-wide amount in controversy exceeds \$5 million, and there are more than 100 putative class members." *Chem. Toxin Working Grp. Inc. v. Johnson & Johnson*, No. 1:22-cv-1259-RCL, 2023 U.S. Dist. LEXIS 50953, at *3 (D.D.C. Mar. 24, 2023).

8. This Court also has subject matter jurisdiction over the federal claim in this action pursuant to 28 U.S.C. § 1331.

Social Security numbers all revealed, TechRadar (Oct. 1, 2026), <https://www.techradar.com/pro/security/massive-pentagon-hack-sees-records-of-2-7-million-us-military-personnel-leaked-during-months-long-data-breach-names-military-service-records-and-social-security-numbers-all-revealed>.

9. This Court also has subject matter jurisdiction over the Privacy Act of 1974 claim pursuant to 5 U.S.C. § 552a(g)(1).

10. This Court has personal jurisdiction because Defendant's principal place of business is located in this District and the relevant conduct occurred in this District.

11. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this District.

12. Venue is also proper in this District under 5 U.S.C. § 552a(g)(5).

PARTIES

A. Plaintiff Tristyn Edwards

13. Plaintiff Tristyn Edwards is a resident and citizen of California, and he brings this action in his individual capacity and on behalf of all others similarly situated. He enlisted in the United States Marine Corps around September 2023. He has continued to work for the U.S. military since then to the present day.

14. Pursuant to his enlistment in the Marine Corps, Mr. Edwards was required to disclose extensive amounts of PII to DOW, which was then stored and maintained by DMDC. In maintaining his PII, Defendants expressly and impliedly promised to safeguard it. Defendants, however, did not take proper care of Mr. Edwards's PII, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures. Mr. Edwards has received emails informing him that his PII is available on the dark web.

15. On or around September 18, 2026, Mr. Edwards was informed by Defendants through a form notice that his PII was compromised by cybercriminals.

16. Prior to receiving this notice but after the Data Breach began, on or about August 20, 2026, Mr. Edwards experienced multiple fraudulent charges on his debit card (amounting to \$317.91 total), despite his diligent efforts to safeguard his debit card information and other PII. At least one of these fraudulent expenses appears to be used for finding more PII through a website called PeopleFinder, which leads him to believe this expenditure may have come from a cybercriminal with access to his PII.

17. Mr. Edwards and Class members have faced and will continue to face a certainly impending and substantial risk of future harm as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include identity theft, fraudulent charges, new lines of credit opened without their permission, targeted advertising without consent, and excess spam calls, texts, and emails.

18. Some of these harms will not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information. Indeed, Mr. Edwards's experience only further underscores the inadequacy of DOW's drastically delayed notice, as he already experienced fraudulent charges before he was even told that his PII had been breached.

19. Mr. Edwards, in particular, must obtain and maintain a security clearance for his work. Certain common mitigatory measures, such as freezing his credit, are not available to him, and the damage to his reputation that could accompany identity theft could impact his employment. He has also suffered a noted increase in spam and junk phone calls and emails.

20. Mr. Edwards greatly values his privacy, especially given his continuing involvement in the military, and he worries that continued dissemination of his PII may result in his facing further fraud that could harm his reputation.

B. Plaintiff Morgan Stampfli

21. Plaintiff Morgan Stampfli is a resident and citizen of New York, and he brings this action in his individual capacity and on behalf of all others similarly situated. He enlisted in the United States Marine Corps in 2010 and remained in the Marine Corps until 2021, at which point he left to pursue other career opportunities.

22. Pursuant to his service in the Marine Corps, Mr. Stampfli was required to disclose extensive amounts of PII to DOW, which was then stored and maintained by DMDC. In maintaining his PII, Defendant expressly and impliedly promised to safeguard it. Defendant, however, did not take proper care of Mr. Stampfli's PII, leading to its exposure to, and exfiltration by cybercriminals as a direct result of Defendant's inadequate security measures.

23. On or around September 18, 2026, Mr. Stampfli was informed by Defendant through a form notice that his PII was compromised by cybercriminals.

24. Mere days after receiving this notice, Mr. Stampfli experienced an unauthorized online purchase from KaTom Restaurant Supply charged to his Navy Federal Credit Union debit card, amounting to \$271.19 total. The fraudulent order contained his correct personal and billing information, including his name, address, telephone number, email address, and debit card information. The purchase was being shipped to an individual and an address that he did not recognize in Illinois. After becoming aware of the unauthorized purchase, he contacted KaTom

and they flagged the transaction as fraudulent. Mr. Stampfli also called Navy Federal Credit Union to cancel the compromised debit card and get a replacement card.

25. Additionally, around September 24 & 25, 2026, Mr. Stampfli's email address was suddenly registered for a large number of unrelated newsletters and mailing lists. This has resulted in him receiving a lot of spam in his email, including emails requesting that he confirm subscriptions to services for which he never signed up.

26. Mr. Stampfli and Class members have faced and will continue to face a certainly impending and substantial risk of future harm as a result of Defendant's ineffective data security measures, as further set forth herein. Some of these harms will include identity theft, fraudulent charges, new lines of credit opened without their permission, targeted advertising without consent, and excess spam calls, texts, and emails. Some of these harms will not materialize for years after the Data Breach, rendering Defendant's notice letter woefully inadequate to prevent the fraud that will continue to occur through the misuse of Class members' information.

27. Mr. Stampfli greatly values his privacy and would not have entrusted his information to the DOW and DMDC had he known that it would not be adequately protected. He fears that continued dissemination of his PII may result in more fraud and more spam.

C. Defendant United States Department of War

28. Defendant DOW is a U.S. agency with headquarters at 1400 Defense Pentagon, Washington, DC 20301-1000. The DOW maintains and oversees the United States military, including the Army, Navy, Air Force, Marine Corps, Space Force, and Coast Guard. As of January 2026, the DOW estimated that it employed approximately 2.8 million civilian and

military personnel.⁶ In order to manage this massive workforce, the DOW created the DMDC to aggregate and analyze data about its personnel.⁷ This includes keeping extensive records on current and former personnel and their families in order to provide benefits and ensure the correct individuals have access to the correct DOW systems.⁸ In Fiscal Year 2024, DMDC held more than 60 million DOW Person Records on servicemembers, civilians, contractors, family members, retirees, and veterans, and it processed more than 1.8 billion transactions for DMDC data sharing.⁹

FACTUAL ALLEGATIONS

A. The Defense Manpower Data Center Collects and Stores a Substantial Amount of Sensitive PII Related to Servicemembers and Military-Affiliated Individuals.

29. In order to aggregate and analyze data regarding the massive military and civilian workforces of the DOW, the DMDC was established under the Under Secretary of Defense for Personnel and Readiness and the Director of Defense Human Resources Activity (“DHRA”).¹⁰ The DMDC “collate[s] personnel, manpower, training, financial, and other data” to “catalogue[] the history of personnel in the military and their family for purposes of healthcare, retirement funding, and other administrative needs.”¹¹

30. The DMDC manages multiple programs for the DHRA and DOW, namely:

⁶ See DOW, Defense Manpower Profile Report: Fiscal Year 2026 at 2, <https://prhome.war.gov/Portals/52/Documents/OED/FY2026%20Annual%20Defense%20Manpower%20Profile%20Report.pdf?ver=jvWlao9RVDRdj0ohfjz7fQ%3D%3D>.

⁷ See DMDC Overview.

⁸ *Id.*

⁹ *Id.*

¹⁰ See U.S. Govt. Accountability Office, DOD Needs to Review Its Defense Agencies and Field Activities for Efficiency and Effectiveness, GAO-26-107781, at 16 (Sept. 3, 2026).

¹¹ DMDC Overview.

- a. Defense Enrollment Eligibility Reporting System (“DEERS”): Operates as the “authoritative eligibility and enrollment repository for manpower, personnel identity, and affiliation data on military, civilians, retirees, family members, and other populations,” and “supports access to DoD benefits such as commissary, exchange, and morale-welfare services for a growing number of current and former [DOW] populations.”¹² This includes sub-programs dedicated to “provid[ing] real-time determination of eligibility for DoD entitlements (including medical, dental, life insurance, education, and commissary programs) and Morale, Welfare and Recreation activities (such as Exchange privileges and recreational activities),” and “provide support for evolving efforts to modernize medical records that can be used across the Federal enclave to support care in facilities managed by DoD, the VA, and other Federal partners.”¹³
- b. Enterprise Human Resource Information System (“EHRIS”): Develops and maintains “systems that support Civilian HR Management...processes across the [DOW],” including those related to “unemployment and injury compensation management; equal employment opportunity (EEO) complaint investigations; labor and employee relations case management; senior

¹² DOW DHRA, *Fiscal Year 2026 Budget Estimates: Operation and Maintenance, Defense-Wide* 6 (2025), https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2026/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/DHRA_OP-5.pdf.

¹³ *Id.* at 7.

executive performance and talent management; strategic human capital management...analysis and planning; and the priority placement program.”¹⁴

- c. Identity Credential Management (“ICM”): “[S]upports identity data updates and the issuance of identification cards to Service members, civilian employees, contractors, retirees and other Federal partners,” such as by “providing the global system of software and hardware that issues official [DOW] ID cards to eligible personnel,” including the RAPIDS/Common Access Cards (“CAC”) that “facilitate[] access to [DOW] bases and installations, [DOW] networks and computers, and [DOW] benefits and entitlements.”¹⁵
- d. Personnel Support Programs (“PSP”): Provides IT services and programs “committed to ensuring the safety, well-being, and support of all [DOW] personnel by delivering accurate and timely information and services,” including through sub-programs that “gather, analyze, and share information on the physical location of [DOW] members and affiliated personnel,” allow authorized personnel to retrieve personnel records of military and civilian employees, track personnel promotion and enlistment, and track contractor resources.¹⁶

31. These programs are offered to a variety of internal stakeholders and external partners of DOW, including the Office of the Secretary of Defense, Combatant Commands, DOW

¹⁴ *Id.* at 10.

¹⁵ *Id.* at 10–11.

¹⁶ *Id.* at 11–13.

World-Wide Enterprise, DOW Investigative Agencies, the uniformed services, other government departments and agencies, and third-party research and industry partners.¹⁷

32. These programs include various systems of records containing sensitive or confidential PII, including social security numbers, financial account information, and healthcare-related information.¹⁸

33. Given the millions of records containing PII about American servicemembers and individuals with close ties to the military, DOW should have known that DMDC systems would be the target of substantial intrusion efforts, whether that be by foreign adversaries or cybercriminals hoping to sell that sensitive PII to foreign adversaries.

34. Even independent of the heightened national security interests at play with PII stored in DMDC systems, cybercriminals have also previously targeted DMDC systems to commit identity theft and wire fraud. *See United States v. Boling, et al.*, Case No. 5:19-cr-00524-OLG, Indictment, ECF No. 3, ¶¶ 8–12 (W.D. Tex.) (describing conspiracy to use DMDC-maintained DS Logon system to steal funds and benefits from the personal bank accounts of military-affiliated

¹⁷ See DMDC Overview.

¹⁸ See, e.g., System of Records Notice: Uniformed Services Human Resources Information System (DMDC01), 91 Fed. Reg. 10,373 (Mar. 3, 2026), <https://www.federalregister.gov/documents/2026/03/03/2026-04170/privacy-act-of-1974-system-of-records>; System of Records Notice: Defense Enrollment Eligibility Reporting System (DEERS) (DMDC02 DoD), 87 Fed. Reg. 32,384 (May 31, 2022), <https://www.federalregister.gov/documents/2022/05/31/2022-11610/privacy-act-of-1974-system-of-records>; Privacy Impact Assessment (PIA) for Defense Personnel Records Information Retrieval System (DPRIS) at 1, https://www.dhra.mil/Portals/52/Documents/Privacy/PIA/DPRIS_PIA.pdf (noting that “[u]sers search DPRIS using name/social security number”); Department of Defense Inspector General, Management Advisory: Reliability of the Defense Enrollment Eligibility Reporting System Data, DODIG-2023-089 at 3 (Jun. 27, 2023), <https://www.oversight.gov/sites/default/files/documents/reports/2023-07/DODIG-2023-089.pdf>.

individuals). This too should have put DOW on notice that DMDC systems would be a high-value target for cybercriminals.

B. DOW and DMDC Failed to Implement Adequate Cybersecurity Safeguards.

35. The Federal Information Security Modernization Act (“FISMA”), 44 U.S.C. § 3551, *et seq.*, governs software system requirements for software systems owned or operated by federal agencies and contractors. As Chief Information Officer of the DOW, Kirsten Davies was under a statutory mandate to “implement an agency-wide information security program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source[.]” 44 U.S.C. § 3554(b); *see also* 44 U.S.C. § 3554(a)(3)(B) (establishing that CIOs are responsible for implementing agency information security programs).

36. Under FISMA, an agency must develop, implement, and maintain a security program that assesses the risks and provides adequate security for the operations and assets of programs and software systems under its control. Specifically, FISMA requires: (1) annual agency program reviews, (2) annual Inspector General evaluations, (3) agency reporting to the Office of Management and Budget (“OMB”) the results of Inspector General evaluations, and (4) an annual OMB report to Congress summarizing the material received from agencies. The OMB uses the reports to help it ensure that the various federal agencies are in compliance with its cybersecurity requirements.

37. In accordance with FISMA, the DOW’s Office of the Inspector General (“OIG”) conducts annual, independent audits of the DOW’s cybersecurity program and practices. The Department of Homeland Security (“DHS”) Office of Cybersecurity and Communications issues

Inspector General FISMA Reporting Instructions. Using these guidelines, the OIG reviews DOW's FISMA compliance strategy and documents the status of its compliance efforts.

38. Pursuant to FISMA, the OIG reviews DOW cybersecurity controls and provides a “maturity rating” for each of twenty different FISMA Core Reporting Metrics. These twenty Core Reporting Metrics are organized into ten cybersecurity “domains,” including:

- a. Cybersecurity Governance: “[A] comprehensive cybersecurity strategy that integrates with organizational operations and is designed to prevent the interruption of activities due to cyber threats or attacks.”¹⁹
- b. Cybersecurity – Supply Chain Risk Management: “[A] systematic process for managing exposure to cybersecurity risk throughout supply chains and developing appropriate response strategies, policies, processes, and procedures.”²⁰
- c. Risk and Asset Management: “[T]he program and processes for managing information security risks to organizational operations (including mission, functions, image, and reputation), organizational assets, staff, and other organizations.”²¹
- d. Configuration Management: “[A] collection of activities focused on establishing and maintaining the integrity of information technology products and information systems.”²²

¹⁹ DOW OIG, Management Advisory: The DoW's FY 2025 Compliance with the Federal Information Security Modernization Act of 2014, Report No. DOWIG-2026-097, at 20 (Jul. 20, 2026), https://media.defense.gov/2026/Jul/20/2003963207/-1/-1/1/DOWIG-2026-097_REDACTED_SECURE.PDF (hereinafter “DOW OIG FY2025 FISMA Report”).

²⁰ *Id.*

²¹ *Id.*

²² *Id.*

- e. Identity and Access Management: “[T]he controls and processes for identifying users, using credentials, and managing users access to network resources.”²³
- f. Data Protection and Privacy: “[T]he controls and processes for protecting systems and information (data) and ensuring that management of those systems and data are consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of information.”²⁴
- g. Security Training: “[A]n established program that ensures all users complete the necessary mandatory cybersecurity training requirements, including specialized training for individuals requiring privileged access.”²⁵
- h. Information Security Continuous Monitoring: “[T]he process for maintaining ongoing awareness of information security, vulnerabilities, and threats to support operational risk management decisions.”²⁶
- i. Incident Response: “[A] formal, focused, and coordinated approach to responding to cybersecurity incidents.”²⁷
- j. Contingency Planning: “[A] coordinated strategy involving plans, procedures, and technical measures that will enable the recovery of information systems, operations, and data after a disruption.”²⁸

39. In the DOW’s Fiscal Year 2025 OIG Report, released only a few days after the Data Breach was discovered, the OIG reported that “DoW officials have not taken the necessary

²³ *Id.*
²⁴ *Id.*
²⁵ *Id.*
²⁶ *Id.* at 21.
²⁷ *Id.*
²⁸ *Id.*

actions to demonstrate that they were operating at an effective level for 14 of the 20 IG FISMA Core metrics.”²⁹ In particular, the OIG noted that “DoW officials did not fully establish an organizational governance structure...for two of the five Supplemental metrics.”³⁰

40. These problems are not new. In the FY2025 OIG Report, the DOW OIG reported that “[t]he DoW’s overall information security program remained ineffective for the last 5 years as defined by IG FISMA reporting metrics guidance.”³¹

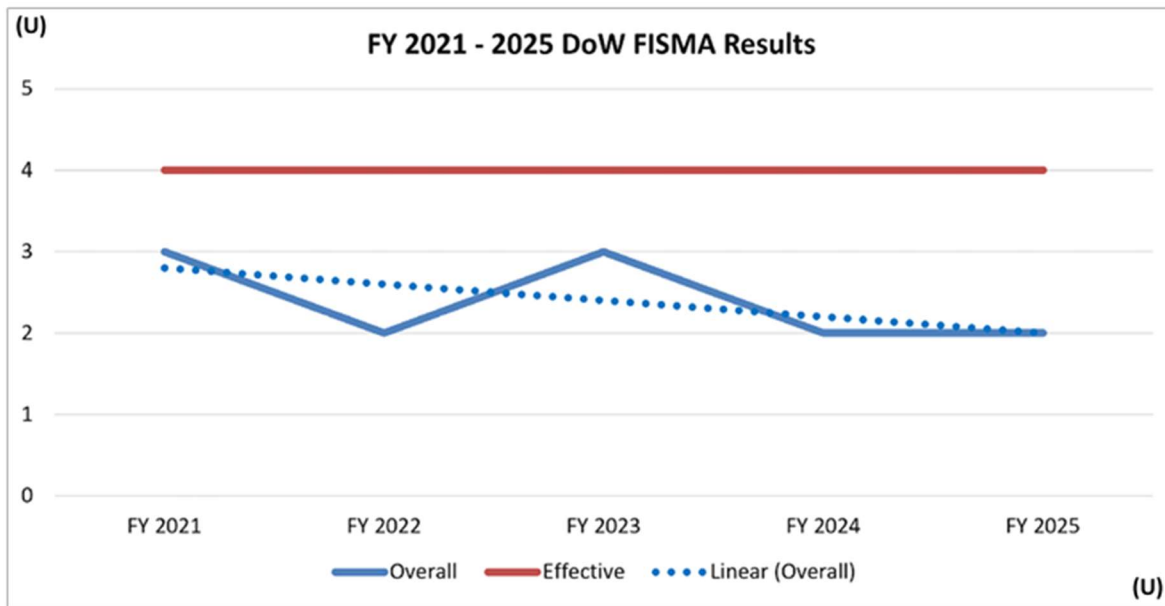


Figure 1: Chart Showing DOW FISMA Non-Compliance from FY2025 OIG Report³²

41. The FY2024 OIG Report provided some greater detail on non-national security systems, including flagging issues with DOW components failing to consistently: (1) “collect self-attestations from third-party software providers to certify that they used NIST secure development practices”; (2) implement the requirements of the Information Security Continuous Monitoring

²⁹ *Id.* at 4. Note that substantial portions of the audit report are redacted, including the specific maturity scores assigned to the different OIG Core metrics, so the specific metrics and deficiencies cannot readily be identified in this report.

³⁰ *Id.* at 6.

³¹ *Id.*

³² *Id.* at 6.

domain; and (3) “implement or report that they implemented all necessary information system controls for its non-national security systems as required by NIST and [DOW] guidance.”³³

42. The FY2024 OIG Report further stated that DOW components “did not consistently implement information system controls for their non-national security systems relating to” metrics focused on Configuration Management (Metrics 20 and 21), Identity and Access Management (Metric 32), Data Protection and Privacy (Metrics 36 and 37), and Contingency Planning (Metrics 61, 62, 63, and 64).³⁴ Particularly relevant here, this indicates failure to consistently implement the following:

- a. Configuration Management Metric 21: Use of “flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities”;³⁵
- b. Identity and Access Management Metric 32: Use of “processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed”;³⁶

³³ Dep’t of Def. OIG, Management Advisory: The DoD’s FY 2024 Compliance with the Federal Information Security Modernization Act of 2014, Report No. DODIG-2025-086, at 10–11, 13 (Apr. 16, 2025), <https://media.defense.gov/2025/Apr/17/2003690664/-1/-1/1/DODIG-2025-086.PDF> (hereinafter “DOD OIG FY2024 FISMA Report”).

³⁴ *Id.* at 14–15.

³⁵ *Id.* at 26.

³⁶ *Id.* at 27.

- c. Data Protection and Privacy Metric 36: Use of “security controls to protect [the component’s] PII and other agency sensitive data, as appropriate, throughout the data lifecycle”³⁷; and
- d. Data Protection and Privacy Metric 37: Use of “security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses.”³⁸

43. The FY2024 and FY2023 OIG Reports twice put DOW on notice of the stakes: “Consistent implementation of cybersecurity policies and procedures is critical for an effective cybersecurity program and reduces the risk of successful cyber attacks, data breaches, data loss, data manipulation, and unauthorized disclosures of mission-essential or sensitive information by malicious actors.”³⁹ Each of these reports called on DOW to correct a number of specific cybersecurity deficiencies shortly after providing this warning.

44. The DMDC also has a history of failing to implement adequate cybersecurity controls. In 2012, the DMDC was specifically subject to an OIG investigation which found that DMDC personnel “did not implement adequate controls for identifying, protecting, and mitigating potential cyber attacks against the DEERS operating system.”⁴⁰ Six years later, in a follow-up audit of DEERS, the OIG reported that four recommendations remained outstanding, including failure to implement “a standard security schedule for scans to verify and document the operational

³⁷ *Id.*

³⁸ *Id.*

³⁹ DOD OIG FY2024 FISMA Report at 1; Dep’t of Def. OIG, Management Advisory: The DoD’s FY 2023 Compliance with the Federal Information Security Modernization Act of 2014, Report No. DODIG-2024-084, at 5 (May 21, 2024), <https://media.defense.gov/2024/May/23/2003471423/-1/-1/1/DODIG-2024-084%20REDACTED%20SECURE.PDF> (hereinafter “DOD OIG FY2023 FISMA Report”) (containing the exact same quoted language).

⁴⁰ Dep’t of Def. OIG, Improvements Needed to Strengthen the Defense Enrollment Eligibility Reporting System Security Posture, Report No. DODIG-2012-090, at 5 (May 22, 2012), <https://media.defense.gov/2019/Aug/22/2002174064/-1/-1/1/DODIG-2012-090.PDF>.

functionality” of certain systems.⁴¹ Later in that report, the OIG cautioned: “If DMDC personnel do not continuously monitor the effectiveness of controls designed and implemented to strengthen the DEERS security posture, hackers can exploit vulnerabilities that jeopardize the integrity and confidentiality of sensitive DEERS data.”⁴² In the OIG’s 2020 Semiannual Report to Congress, it noted that the DMDC still had not completed its recommendation from the 2018 DEERS Report to implement a centralized procedure for out-processing terminated personnel.⁴³

45. DMDC’s failure to protect PII on its systems persists even in more recent months. In August 2026, the DOW confirmed that “[a]bout 215,000 active-duty and reserve troops—about 10% of the total force—were out of compliance with the security rules needed to hold a Common Access Card.” Common Access Cards and their underlying documentation are managed by DMDC in conjunction with its DEERS system. Common Access Cards of this kind can “give holders access to military installations, secure networks and other essential services” at DOW.⁴⁴ The failure of DMDC to police these identification cards, which could allow bad actors to access sensitive PII about millions of servicemembers and their families, reflects the DOW’s continued failure to safeguard the information that was breached.

⁴¹ Dep’t of Def. OIG, Followup Audit: The Defense Enrollment Eligibility Reporting System Security Posture, Report No. DODIG-2018-096, at I (May 30, 2018), <https://media.defense.gov/2018/Apr/12/2001902705/-1/-1/1/DODIG-2018-096.PDF>.

⁴² *Id.* at 12.

⁴³ Dep’t of Def. OIG, Semiannual Report to the Congress: April 1, 2020 Through September 30, 2020, at 143 (2020), <https://www.oversight.gov/sites/default/files/documents/reports/2020-12/DOD%2520OIG%2520SEMIANNUAL%2520REPORT%2520TO%2520THE%2520CONGRESS%2520APRIL%25201%2C%25202020%2520TO%2520SEPTEMBER%252030%2C%25202020.pdf>.

⁴⁴ See Rachel S. Cohen, *Pentagon finds ID problems affecting 215,000 troops*, Federal News Network (Sept. 8, 2026), <https://federalnewsnetwork.com/defense-main/2026/09/pentagon-finds-id-problems-affecting-215000-troops/>.

C. The Data Breach Leads to Disclosure of Sensitive PII for Military-Adjacent Individuals for More Than Nine Months, and DOW Delays Notice to Affected Individuals.

46. In mid-September 2026, Defendant began sending data breach notification letters out to a variety of individuals either in or affiliated with the U.S. military. The letters read as follows:

The Defense Manpower Data Center (DMDC), a component of the Department of War (DoW), is writing to inform you of a breach of a DMDC information system, which involved your personally identifiable information (PII). The DoW understands the importance of maintaining the privacy and security of your PII, which is why we are contacting you to offer credit monitoring services and inform you about steps you can take to protect your information.

What Happened

On July 16, 2026, a security vulnerability in a DMDC file sharing system was discovered, which allowed unauthorized users to access files. DMDC immediately updated the file sharing system to patch the vulnerability and the system was restored.

What Information Was Involved

Analysis identified that between October 2025 and the date of discovery, a small number of unauthorized users accessed files on a server containing unencrypted PII. The types of PII involved vary by individual; however, in your case, they include social security number (SSN) and at least one additional identifier such as name, date of birth, contact information, sex, race, and military personnel information (such as occupational specialty). At this time, DoW does not have any indications of misuse of the accessed information.

What We Are Doing

Upon discovery of the security vulnerability, DMDC immediately initiated privacy and cybersecurity incident response actions in accordance with Office of Management and Budget and Department guidelines and policies. We are taking appropriate actions to assess and enhance the cybersecurity posture of the DMDC system....

47. Mr. Edwards and Mr. Stampfli received these letters on September 18, 2026, which included a QR code and link for him to enroll in 12 months of free credit monitoring services through the company IDX.

48. Shortly after the first notice letters were sent out, on September 28, 2026, the DOW confirmed that a breach of the DMDC's information system led to the exposure of PII for about 2.8 million living individuals and 294,000 deceased individuals.⁴⁵

49. DOW has offered no explanation for the *nine month* delay between the beginning of the breach and its discovery in July 2026. Worse still, it has offered no information explaining the two months of additional delay between discovery of the breach and the sending of notices to affected individuals.

50. Defendants' failure to timely detect the unauthorized intrusion and send adequate notice to impacted individuals resulted in Plaintiffs and Class members suffering harm they otherwise could have avoided had a timely disclosure been made. Indeed, Mr. Edwards himself could have taken steps to avoid the fraudulent charges on his financial accounts had he known his information had been subject to a breach months prior.

51. Defendant's notice of the Data Breach was not just untimely but woefully deficient. The notice failed to provide basic details, including, but not limited to: what system was actually infiltrated, how unauthorized parties accessed the DMDC's networks, how DMDC learned of the Data Breach, whether the PII of affected individuals had been exfiltrated from the system, whether the Breach occurred system-wide, and how many users were affected by the Data Breach.

52. To date, DOW has refused to identify the specific system of records breached, referring only to a general "DMDC file sharing system." Nonetheless, the fact that the DOW was

⁴⁵ See Cohen Data Breach Article.

able to identify the specific individuals impacted by the Data Breach and the specific categories of data leaked for each individual, considered together with the various systems of records managed by the DMDC,⁴⁶ suggests that the Data Breach impacted a system of records as defined by the Privacy Act. The precise identity of the compromised system and the Defendant's practices for retrieving records from that system are facts exclusively within the Defendant's possession and control.

53. Nor does the notice provide a clear explanation of the risk Plaintiffs and Class members face as a result of the loss of their Private Information. The notice only recommends that Class members take advantage of one year of free credit monitoring, but this is far from an adequate remedy. Credit monitoring only alerts individuals to the misuse of their information after it happens, which might not take place until years after the Data Breach. The notice also included a document from IDX recommending that affected individuals review their credit reports and place fraud alerts through major credit bureaus, but this is insufficient for the same reasons. The only other recommendation made in the IDX form is to place a security freeze on accounts, but even then IDX acknowledges that such an approach will prevent the impacted individual from being able to borrow money, obtain instant credit or get a new credit card, which places a significant financial burden on victims of the breach unless they lift or permanently remove the freeze, which would once again leave them vulnerable.

D. Defendant Willfully and Intentionally Disregarded the Substantial Risk of a Data Breach by Failing to Implement Reasonable and Adequate Cybersecurity Safeguards.

54. The fact that the breach of DMDC systems went completely unnoticed for almost nine months reflects a startling lack of cybersecurity controls and system monitoring. Public

⁴⁶ See supra note 18 (listing out a variety of DMDC systems of records).

cybersecurity commentators have noted that the Data Breach “wasn’t the result of sophisticated cyberattack. It was a failure of fundamental security controls – encryption, access management and monitoring – at an organization that helps set cybersecurity standards for the entire federal government.”⁴⁷ Other commentators have compared this breach to the 2015 breach of the Office of Personnel Management, which involved intruders first accessing government systems about two years before detection.⁴⁸

55. The nine-month long intrusion into DMDC systems reflects insufficient monitoring of system logs and a failure to maintain appropriate access controls. At the very least, the length of access by unauthorized users “suggests that whatever monitoring existed did not identify repeated or sustained retrieval of sensitive files.”⁴⁹

56. Indeed, internal DOW policies require IT system owners “to review audit logs for inappropriate and suspicious activity at least weekly and report security incidents and violations.”⁵⁰ The fact that substantial amounts of data were accessed without proper authorization for nearly nine months suggests flagrant disregard for this policy by Defendant.

57. The types of data accessed through the Data Breach are particularly valuable to cybercriminals, as it can “help attackers identify government personnel and tailor attempts to deceive them through fraud schemes. Such data can also identify employees whose work is of

⁴⁷ Richard Livingston, *Pentagon breach exposes failure to follow its own standards*, techtarget (Oct. 8, 2026), <https://www.techtargget.com/cybersecurity/news/366652020/Pentagon-breach-exposes-failure-to-follow-its-own-standards>.

⁴⁸ Cloud Security Alliance AI Safety Initiative, *Nine Months Inside: The Pentagon DMDC Personnel Data Breach*, CSA Lab Space (Oct. 5, 2026), <https://labs.cloudsecurityalliance.org/research/csa-research-note-dmdc-long-dwell-personnel-data-20261005-cs> (hereinafter “Cloud Security Alliance Report”).

⁴⁹ *Id.*

⁵⁰ Dep’t of Def., DOD Instruction 8520.04: Access Management for DOD Information Systems § 4.4(b)(3), at 22 (Sept. 3, 2024), <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852004p.pdf>.

particular interest to foreign intelligence services.”⁵¹ Indeed, “[a] record exposed in 2025 can remain useful years later to an adversary willing to wait, for identity fraud, targeting, and social engineering. The inclusion of occupational details in some records raises the possibility of use in counterintelligence or targeting contexts[.]”⁵²

58. In light of the types of personal information at issue, it is highly likely that the PII accessed on DMDC’s systems was specifically targeted by cybercriminals with the intent to steal and misuse it. This also suggests that the PII is being sold on the dark web—a fact further supported by the fact that some individuals facing PII leakage, like Mr. Edwards and Mr. Stampfli, have already experienced actual fraud or notifications that their data was leaked on the dark web. This means that unauthorized parties have accessed, viewed, and exfiltrated Plaintiffs’ and Class members’ unencrypted, unredacted, sensitive personal information, including names, addresses, Social Security numbers, and more as a result of Defendant’s lax data security practices and protocols.

59. Some commentators have also noted that the unencrypted nature of the PII leaked in the Data Breach suggests that numerous typical cybersecurity measures were not taken. The Cloud Security Alliance noted in their assessment of the breach that “[f]ield level protection of Social Security numbers, or tokenization that keeps them out of exchange files altogether, would likely have reduced the impact [of the Data Breach] more directly.”⁵³

60. The Breach occurred because Defendant intentionally and willfully failed to take appropriate measures to protect the PII it collected and stored. Among other things, Defendant

⁵¹ David DiMolfetta, *Pentagon, FBI personnel-data beaches raise questions* (Oct. 5, 2026), <https://www.defenseone.com/threats/2026/10/pentagon-personnel-data-breach-went-undetected-months/416421>.

⁵² See Cloud Security Alliance Report.

⁵³ *Id.*

failed to implement data security measures designed to prevent this attack, despite repeated warnings about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on other government agencies.

61. Defendant disregarded the rights of Plaintiffs and Class members by intentionally and willfully failing to take and implement adequate and reasonable measures to ensure that Plaintiffs' and Class members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the monitoring and encryption of data. As a result of Defendant's conduct, the PII of Plaintiffs and Class members was compromised through unauthorized access by an unknown third party. Plaintiffs and Class members have a continuing interest in ensuring that their information is and remains safe.

E. Plaintiffs and Class Members Have Suffered Damages as a Result of the Data Breach.

62. Due to Defendants' willful, intentional, and flagrant disregard of Plaintiffs' and Class members' privacy rights, and the DOW's failure to fully implement the recommendations and instructions of the OIG, Plaintiffs and Class members have suffered and will continue to suffer damages, including actual damages within the meaning of the Privacy Act, pecuniary losses, anxiety, and emotional distress. They have suffered or are at increased risk of suffering from:

- a. the loss of the opportunity to control how their PII is used;
- b. the diminution in the value and/or use of their PII entrusted to the DOW for the purpose of deriving employment or benefits from the DOW and with the understanding that the DOW and its contractors would safeguard their PII against theft and not allow access and misuse of their PII by others;
- c. the compromise, publication, and/or theft of their PII and the PII of their family

- members, neighbors, and acquaintances;
- d. out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts;
 - e. lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to efforts spent researching how to prevent, detect, contest, and recover from PII misuse;
 - f. costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports, and assets;
 - g. unauthorized use of compromised PII to open new financial and/or health care or medical accounts;
 - h. the continued risk to their PII, and the PII of their family members and acquaintances, which remains in the DMDC's possession and is subject to further breaches so long as the DOW fails to undertake appropriate and adequate measures to protect PII in its possession; and
 - i. current and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Class members and their families.

63. The fact that Plaintiffs' and Class members' Private Information was stolen means that Class members' information is likely for sale by cybercriminals and will be misused in additional instances in the future.

64. At all relevant times, Defendants were well aware that Private Information they collect from Plaintiffs and Class members is highly sensitive and of significant value to those who would use it for wrongful purposes.

65. Most salient here are the security implications of Private Information being leaked about servicemembers and their families, which presents unique security risks.

66. Servicemembers and their families are particularly valuable targets for cyber operations. In early September, Chris Olson of The Media Trust reported that “[b]etween July 2025 and July 2026, we observed a dramatic increase in AI-enabled phishing campaigns targeting 277 domestic military bases, representing approximately 99 percent of all US military installations, along with military personnel and families living on base. Monthly attack volume climbed from hundreds of thousands of events to more than 4.3 million attacks in July 2026, the highest level ever recorded during the monitoring period.”⁵⁴ This time frame aligns with the duration of the Data Breach.

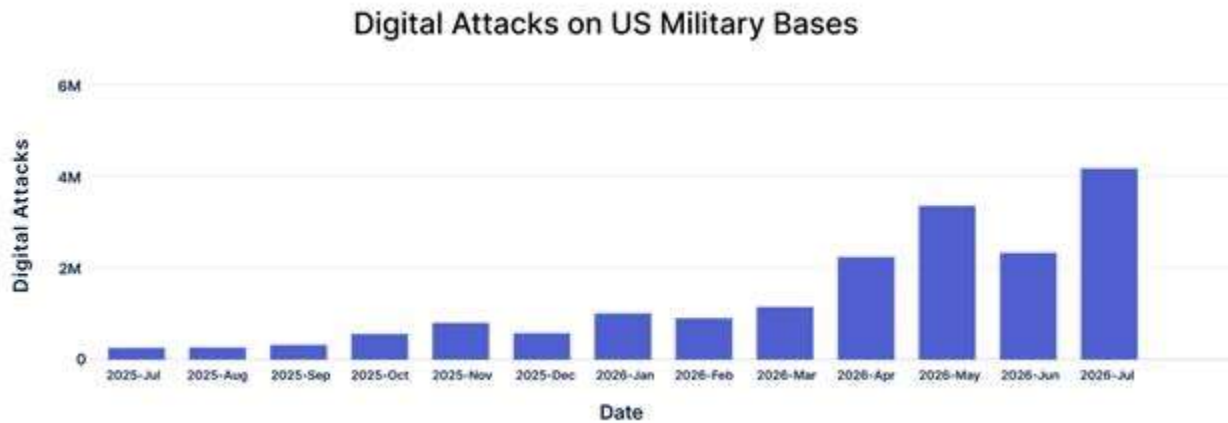


Figure 2: Chart from *TheDefensePost* Article on Increasing Digital Attacks on US Military⁵⁵

⁵⁴ Chris Olson, *Phishing Campaign Targets 99% of US Military Bases During Heightened US-Iran Tensions*, *TheDefensePost* (Sept. 8, 2026), <https://thedefensepost.com/2026/09/08/media-trust-ai-phishing/>.

⁵⁵ *Id.*

67. Olson noted: “Military families are not incidental victims. They are part of the attack surface. Adversaries recognize that compromising people is often easier than compromising military networks. If they cannot reach the mission directly, they target the people connected to it.”⁵⁶

68. Compromising servicemembers and their families by using leaked Private Information can take many forms. In some instances, servicemembers and their families have received direct threats from foreign adversaries—a problem so bad that the U.S. Navy circulated a memorandum in April 2026 providing sailors information on how to secure their digital accounts to prevent further issues.⁵⁷ In one reported instance, members of an adversary group showed up at hotels in Gulf countries inquiring about U.S. servicemembers temporarily staying there, forcing those servicemembers to relocate for safety.⁵⁸

69. Setting aside the security threats faced by servicemembers and their families following a data breach, military families are also uniquely vulnerable to fraud, whether that comes through job scams sent to military spouses or romance scams directed at servicemembers themselves.⁵⁹ This further shows that the failure of DMDC to protect the PII of servicemembers and their families prior to the Data Breach may now result in imminent harm to those individuals.

70. Even absent the military nexus of the Private Information at issue in the Data Breach, PII is a generally valuable commodity to identity thieves. As the FTC has recognized,

⁵⁶ *Id.*

⁵⁷ Karen Jowers, ‘Scary and silencing’: Troops, families receive threats from foreign bad actors, *MilitaryTimes* (May 29, 2026), <https://www.militarytimes.com/news/pentagon-congress/2026/05/29/scary-and-silencing-troops-families-receive-threats-from-foreign-bad-actors/>.

⁵⁸ *Id.*

⁵⁹ Karen Jowers, *Rampant attempts to defraud troops warrants crack down, advocates say*, *FederalTimes* (Jan. 27, 2026), <https://www.federaltimes.com/federal-oversight/2026/01/27/rampant-attempts-to-defraud-troops-warrants-crack-down-advocates-say/>.

identity thieves can commit an array of crimes including identity theft, medical fraud, and financial fraud.⁶⁰ Indeed, a robust “cyber black market” exists in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the dark web.

71. Research shows that full identity packets (SSN, DOB, etc.) can sell on dark web markets for significant sums, reflecting high demand.⁶¹

72. The ramifications of Defendant’s failure to keep Plaintiffs’ and Class members’ Private Information secure are long-lasting and severe. Once Private Information is stolen, fraudulent use of that information and damage to victims may continue for years. In addition, as technology advances, computer programs may scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible. This is known as the “mosaic effect,” and it creates unique privacy concerns for private individuals. It also diminishes the value of Plaintiffs’ and Class members’ Private Information.

73. Further, as a direct result of Defendant’s intentional and willful misconduct that resulted in the Data Breach, the unauthorized parties that were able to access, acquire, and view the Private Information are now equipped to engage in identity theft and misuse of Plaintiffs’ and Class members’ Private Information as detailed above, and Plaintiffs and members of the Class are at a heightened and increased substantial risk of suffering such identity theft and fraud.

74. In the case of the named Plaintiffs, these risks are not merely theoretical. Both Plaintiffs have reported fraudulent charges made on their financial accounts and one also

⁶⁰ Fed. Trade Comm’n, *How to Tell if Someone is Using Your Identity*, FTC Consumer Advice (Feb. 1, 2022), <https://consumer.ftc.gov/consumer-alerts/2022/02/how-tell-if-someone-using-your-identity>.

⁶¹ Mohammed Khalil, *Dark Web Data Pricing 2025: Real Costs of Stolen Data & Services*, DeepStrike (Aug. 24, 2026), <https://deepstrike.io/blog/dark-web-data-pricing-2025>.

confirmed that his Private Information has been released upon the dark web.

75. The risks associated with identity theft are serious. While some identity theft victims can resolve their problems quickly, others spend hundreds to thousands of dollars and many days repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.

76. The U.S. Department of Justice’s Bureau of Justice Statistics has found that “among victims who had personal information used for fraudulent purposes, twenty-nine percent spent a month or more resolving problems” and that “resolving the problems caused by identity theft [could] take more than a year for some victims.”⁶²

77. Moreover, Plaintiffs and the Class have suffered and continue to face a substantial risk of suffering further out-of-pocket fraud losses such as additional fraudulent charges on online accounts, credit card fraud, applications for benefits made fraudulent in their names, loans opened in their names, medical services billed in their names, and identity theft.

78. The theft of Social Security Numbers is particularly detrimental to victims. The U.S. Social Security Administration (“SSA”) warns that “[i]dentity theft is one of the fastest growing crimes in America.”⁶³ The SSA has stated that “[i]dentity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don’t pay the bills, it damages your credit. You may not find out that someone is using your

⁶² See U.S. Dep’t of Justice, *Victims of Identity Theft*, Office of Justice Programs: Bureau of Justice Statistics 1 (Nov. 13, 2017), <https://www.bjs.gov/content/pub/pdf/vit14.pdf>.

⁶³ *Identity Theft and Your Social Security Number*, SOCIAL SECURITY ADMIN. (Dec. 2013), <http://www.ssa.gov/pubs/EN-05-10064.pdf>.

number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought.”⁶⁴ In short, “[s]omeone illegally using your Social Security number and assuming your identity can cause a lot of problems.”⁶⁵

79. In fact, a new Social Security number is substantially less effective where “other personal information, such as [the victim’s] name and address, remains the same” and for some victims, “a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under your new number may make it more difficult for you to get credit.”⁶⁶

80. Plaintiffs may incur and Class members may have already incurred out of pocket costs for protective and/or responsive measures, such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly attempting to mitigate any harm that may arise from the Data Breach.

81. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding Private Information and of the foreseeable consequences if its data security systems were breached, including the significant costs that would be imposed on impacted individuals as a result of any breach. Indeed, the U.S. Army has itself recognized the consequences of data breaches like this one.⁶⁷

82. Plaintiffs and Class members provided their Private Information to the Defendants with the reasonable expectation and mutual understanding that Defendants would comply with

⁶⁴ *Id.*

⁶⁵ *Id.*

⁶⁶ *Id.*

⁶⁷ See Marti Yoshida, *Protecting your personal information from exploitation*, U.S. Army (Aug. 20, 2024), https://www.army.mil/article/279049/protecting_your_personal_information_from_exploitation.

their obligation to keep such information confidential and secure from unauthorized access. The Data Breach shows that Defendants failed to live up to those expectations, and the above factors, among others, will cause Plaintiffs and Class members harm as a result of that failure.

83. Had Defendant remedied the deficiencies in its data security systems flagged by the DOW OIG over the past five years and properly followed the cybersecurity practices required by DOW's own internal policies, the Data Breach could have been prevented and, ultimately, the theft of Plaintiffs' and Class members' Private Information could never have occurred.

84. As a direct and proximate result of Defendant's wrongful actions and inactions, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives.

85. In addition to a remedy for the economic harm, Plaintiffs and Class members maintain an undeniable interest in ensuring that their Private Information remains secure and is not subject to further misappropriation and theft.

CLASS ACTION ALLEGATIONS

86. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

87. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Federal Rule of Civil Procedure 23(a), 23(b)(1), 23(b)(3), and/or 23(c)(4).

88. Specifically, Plaintiffs bring this action on behalf of the following Nationwide Class:

Nationwide Class

All natural persons whose PII was accessed without authorization as a result of the Data Breach discovered on July 16, 2026, and recognized by DOW on September 28, 2026.

Excluded from the Class are the DOW, as well as agents, officers, and directors (including family members) of the DOW. Also excluded are any judicial officers presiding over this matter and the members of their immediate families and judicial staff. Plaintiffs reserve the right to modify, change, amend, or expand the definition of the Nationwide Class based upon discovery and further investigation.

89. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

90. **Numerosity—Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous that joinder of all Class members would be impracticable. On information and belief, the Nationwide Class includes more than 2.8 million living individuals and 294,000 deceased individuals.⁶⁸

91. **Commonality and Predominance—Federal Rules of Civil Procedure 23(a)(2) and 23(b)(3).** Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual members of the Class. Such common questions of law or fact include, *inter alia*:

- a. Whether the DOW's conduct violated the Privacy Act of 1974;
- b. Whether the DOW failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to

⁶⁸ See Cohen Data Breach Article.

protect against known and anticipated threats or hazards to the security and integrity of these records;

- c. Whether the DOW disclosed Plaintiffs and Class members' PII without their prior written consent;
- d. Whether the DOW's conduct was willful or with flagrant disregard for the security of Plaintiff and Class members' PII;
- e. Whether Plaintiffs and Class members are entitled to damages under the Privacy Act.

Defendant engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and other members of the Class. Similar or identical legal violations, cybersecurity practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that predominate in this action.

92. **Typicality—Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, all Class members were similarly injured through Defendant's uniform misconduct described above and were thus all subject to the Data Breach alleged herein. Further, there are no defenses available to Defendant that are unique to Plaintiffs.

93. **Adequacy of Representation—Federal Rule of Civil Procedure 23(a)(4).** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class they seek to represent, they have retained counsel competent and experienced in complex class action litigation, and they will prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiffs and their counsel.

94. **Superiority—Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the Class are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Class to individually seek redress for Defendant’s wrongful conduct. Even if members of the Class could afford individual litigation, the court system could not. Individualized litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

VIOLATION OF THE PRIVACY ACT OF 1974, 5 U.S.C. § 552a (On Behalf of Plaintiffs and the Nationwide Class)

95. Plaintiffs fully incorporate by reference all of the above paragraphs, as though they are fully set forth herein.

96. The DOW is an “agency” within the meaning of the Privacy Act. 5 U.S.C. § 552a(a)(1) (referencing the definition in 5 U.S.C. § 552(f)).

97. Pursuant to 5 U.S.C. § 552a(e)(10), each agency that maintains a system of records shall “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”

98. The DOW obtained and preserved Plaintiffs’ and Class members’ PII, including SSNs and other sensitive information, in a system of records pursuant to Plaintiffs’ and Class members’ employment by or other military-adjacent relationship with DOW.

99. The DOW is therefore responsible for establishing appropriate “safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity” under 5 U.S.C. § 552a(e)(10).

100. The DOW is, and at all relevant times was, required by law to comply with FISMA. The DOW is also responsible for ensuring that its cybersecurity systems comply with 5 U.S.C. § 552a and other rules and regulations governing cybersecurity practices.

101. However, dating back to at least 2021, through a continuous course of conduct, the DOW intentionally, willfully, and with flagrant disregard failed to comply with FISMA and failed to implement adequate cybersecurity governance mechanisms.⁶⁹ The OIG told DOW in these reports that such governance systems were necessary to “reduce[] the risk of successful cyber attacks, data breaches, data loss, data manipulation, and unauthorized disclosures of mission-essential or sensitive information by malicious actors.”⁷⁰ Despite these warnings, DOW continues to intentionally, willfully, and flagrantly disregard its cybersecurity responsibilities.

102. Specifically, and relevant here, DOW components revealed in the FY2024 OIG Report that “they did not consistently implement information system controls for their non-national security systems relating to” metrics focused on Configuration Management (Metrics 20 and 21), Identity and Access Management (Metric 32), Data Protection and Privacy (Metrics 36

⁶⁹ See, e.g., DOW OIG FY2025 FISMA Report; DOD OIG FY2024 FISMA Report; DOD OIG FY2023 FISMA Report.

⁷⁰ See DOD OIG FY2024 FISMA Report at 1; DOD OIG FY2023 FISMA Report at 5.

and 37), and Contingency Planning (Metrics 61, 62, 63, and 64).⁷¹ Particularly relevant here, this indicates failure to consistently implement the following:

- a. Configuration Management Metric 21: Use of “flaw remediation processes, including asset discovery, vulnerability scanning, analysis, and patch management, to manage software vulnerabilities”;⁷²
- b. Identity and Access Management Metric 32: Use of “processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed”;⁷³
- c. Data Protection and Privacy Metric 36: Use of “security controls to protect [the component’s] PII and other agency sensitive data, as appropriate, throughout the data lifecycle”⁷⁴; and
- d. Data Protection and Privacy Metric 37: Use of “security controls (e.g., EDR) to prevent data exfiltration and enhance network defenses.”⁷⁵

103. Had DOW properly implemented standard cybersecurity controls—such as regular review of accounts, scanning for vulnerabilities, field encryption or tokenization of sensitive PII like SSNs, and routine monitoring of system logs for suspicious activity—the Data Breach could have been avoided. By failing to implement such standard cybersecurity controls

⁷¹ DOD OIG FY2024 FISMA Report at 14–15.

⁷² *Id.* at 26.

⁷³ *Id.* at 27.

⁷⁴ *Id.*

⁷⁵ *Id.*

for sensitive DMDC systems, cybercriminals were granted almost nine months of access to the PII of Plaintiffs and Class members.

104. Through DOW's continuous course of conduct described above, it willfully, intentionally, and with flagrant disregard for the privacy interests of servicemembers and other military-adjacent individuals refused to take steps to implement "appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity," as required by the Privacy Act.

105. The DOW's history of persistent, knowing non-compliance with FISMA's legal requirements ultimately resulted in the "substantial harm, embarrassment, inconvenience, or unfairness" that 5 U.S.C. § 552a(e)(10) is designed to protect against.

106. As a result of the Defendants' conduct, Plaintiffs and Class members have suffered and will continue to suffer actual damages and pecuniary losses within the meaning of the Privacy Act. Such damages have included or may include, without limitation: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to the DOW for the purpose of deriving employment or other benefits from the DOW and with the understanding that the DOW and its contractors would safeguard their PII against theft and not allow access and misuse of their PII by others; (3) the compromise, publication, and/or theft of their PII and the PII of their family members, neighbors, and acquaintances; (4) out-of-pocket costs associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of financial and medical accounts; (5) lost opportunity costs associated with effort expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but

not limited to efforts spent researching how to prevent, detect, contest and recover from identity and health care/medical data misuse; (6) costs associated with the ability to use credit and assets frozen or flagged due to credit misuse, including complete credit denial and/or increased costs to use credit, credit scores, credit reports and assets; (7) unauthorized use of compromised PII to open new financial and/or health care accounts; (8) unauthorized use of compromised PII to improperly and without authorization use the financial and/or health care accounts of Plaintiffs and Class members; (9) the continued risk to their PII, and the PII of their family members, neighbors, and acquaintances, which remains in the DOW's possession and is subject to further breaches so long as the DOW fails to undertake appropriate and adequate measures to protect the PII in its possession; and (10) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of the Class members and their families. Plaintiffs and Class members are thus entitled to relief pursuant to 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the other members of the Class proposed in this Complaint, respectfully demand a jury trial of all issues so triable and requests that the Court enter judgment in their favor and against Defendant, as follows:

- a. Declaring that this action is a proper class action, certifying the Classes as requested herein, designating Plaintiffs as Class Representatives, and appointing Class Counsel as requested in Plaintiffs' expected motion for class certification;
- b. Awarding Plaintiffs and Class members appropriate relief, including actual and statutory damages;
- c. Awarding all attorneys' fees and litigation costs to Plaintiffs and their counsel;

- d. Awarding both pre- and post-judgment interest on any amounts awarded;
and
- e. Ordering such other and further relief as may be just and proper.

JURY DEMAND

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

Date: October 20, 2026

Respectfully submitted,

/s/ Jason S. Rathod

Jason S. Rathod (DC Bar # 1000882)

Nicholas A. Migliaccio (DC Bar # 484366)

MIGLIACCIO & RATHOD, LLP

412 H Street NE

Washington, D.C. 20002

202.470.3520

jrathod@classlawdc.com

nmigliaccio@classlawdc.com