UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

VIETNAM VETERANS OF AMERICA; VIETNAM VETERANS OF AMERICA NEW YORK STATE COUNCIL; VIETNAM VETERANS OF AMERICA CHAPTER 77; and THOMAS BARDEN, Plaintiffs, v. DEPARTMENT OF DEFENSE; JIM MATTIS, Secretary of Defense; DANA W. WHITE, Assistant to the Secretary of Defense for Public Affairs; ANTHONY M. KURTA, Acting Under Secretary of Defense for Personnel and Readiness; WILLIAM H. BOOTH, Director of the Defense Human Resources Activity; MICHAEL V. SORRENTO, Director of the Defense Manpower Data Center, in their official capacities; and the UNITED STATES. Defendants.	Case No. 17-cv-730

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF AND DAMAGES

Plaintiffs Vietnam Veterans of America ("VVA"), Vietnam Veterans of America New York State Council ("VVA NYSC"), Vietnam Veterans of America Chapter 77 ("Chapter 77"), and Thomas Barden, through their undersigned counsel, allege:

INTRODUCTION

1. The Department of Defense ("DoD") operates an online portal (the "SCRA Website" or "Website") that is currently exposing private details about the military service of millions of veterans to anybody at all, anonymously, for any purpose.

2. By making this private information freely accessible, the Defendants are putting veterans at risk of impostor scams, identity theft, and other frauds. Defendants are also depriving veterans their ability to control who learns sensitive details about their military service.

3. Plaintiffs bring this action in order to end this systematic infringement of veterans' privacy, which violates the federal Privacy Act.

4. The SCRA Website allows anyone to search for details about an individual simply by inputting a name and date of birth, or name and Social Security Number ("SSN"). Because nearly everyone's date of birth can easily be obtained on the internet, the SCRA Website permits easy access to information about essentially all veterans or servicemembers in the system.

5. If a query returns a match on DoD's personnel database, the Website discloses the following personal details (collectively, the "Private Information"): (1) the specific dates on which an individual began and ended active duty service; (2) the specific dates, if any, on which a reservist, guardsman or other individual not currently on active duty has been called-up for future active duty; (3) the specific component of the military in which an individual served; and (4) confirmation that the individual served on active duty. If the search is run using a name and SSN, a positive result also serves to confirm that the name and SSN match.

6. Defendants have configured the Website to allow access to the Private Information on a truly massive scale. According to DoD, the Website receives approximately 2.3 billion search queries every year. A single user can submit 250,000 unique searches in a single batch, and up to 12.5 million searches per day. The Website does not ask users to provide their name or contact information and does not ask users to disclose their purpose in seeking to obtain a veteran's Private Information.

7. By leaving Private Information essentially unsecured in this way, Defendants are exposing millions of veterans and servicemembers to significant risks of impostor fraud. Armed with the Private Information, con artists can readily impersonate representatives of government agencies or other trusted organizations. They can obtain a veteran's confidence by discussing details about the veteran's service that only the government or another authorized institution should have.

8. Scammers can also use the SCRA Website to perpetrate forms of identity theft. Private third-parties currently exploit the SCRA Website as a means to authenticate an individual's status as a veteran or servicemember. Those third parties typically demand that veterans turn over their SSN in order to run a search on the Website. By permitting searches using the SSN by anyone and for any purpose, Defendants are incentivizing and effectively encouraging veterans and servicemembers to turn over their SSNs to third parties. This creates a significant and unnecessary risk of identity theft and other frauds.

9. Some third-party companies, such as ID.me, GovX, and SheerID, issue digital credentials purporting to verify a person's identity and veteran status. These services run searches against the SCRA Website in order to grant these digital credentials. This use of the SCRA Website is not permitted by law or regulation. Scammers may take advantage of these private online verification services to obtain fake digital credentials by providing someone else's name and DOB (or SSN).

10. The risk to veterans is real. Plaintiff Thomas Barden, a 21-year veteran of the Air Force and member of VVA, was personally targeted by scammers who were armed with details about his military service that are accessible through the website. Using those details, the scammers gained Mr. Barden's trust and conned him into purchasing fraudulent computer

security software. Months later, the scammers took control of his computer and locked him out of his files unless he paid a ransom, which he refused to do. Mr. Barden continues to be harassed by the same scammers. The experience has cost Mr. Barden money, time, and his computer, not to mention significant anxiety and stress.

11. Mr. Barden's ordeal is no aberration. The federal government has documented that veterans face a disproportionate risk of becoming victims of impostor frauds, identity theft, and other scams. Yet DoD is fueling the problem by allowing scammers to access Private Information about millions of veterans.

12. The SCRA Website also deprives veterans the ability to control access to details about their military service that they often have good reason to keep private. Veterans may face social stigma, discrimination in employment, and other harms on account of their status as former servicemembers. Veterans from the Vietnam Era, in particular, have experienced the sting of rejection and public scorn on account of their service. As a result, many Vietnam-era veterans have sought for years carefully to limit who learns about their service. The SCRA Website essentially takes this choice out of veterans' hands.

13. There is no reason for Defendants to make veterans' Private Information so easily accessible. According to DoD, the SCRA Website is meant to be used for only one limited purpose: to determine whether someone is protected by the Servicemember Civil Relief Act (SCRA), which shields servicemembers on active duty (and certain others) against foreclosure, eviction, and other adverse actions at the hands of banks, landlords, and similar entities.

14. Plaintiffs have no objection to limited disclosure of information for legitimate SCRA purposes. Indeed, it makes good sense to have an efficient way for businesses subject to the SCRA to determine whether a client is protected by that law. But the SCRA Website does not

limit access only to SCRA-covered entities, nor does it limit access for SCRA-related purposes. To the contrary, the SCRA Website does not limit access in any meaningful way.

15. Defendants are violating the Privacy Act, which does not allow Defendants to make private information freely accessible to anyone for any purpose, or to disclose information without keeping track of who they have given it to. Defendants are also violating the Federal Information Security Modernization Act ("FISMA"), which requires Defendants to comply with policies that strictly limit the use of SSNs.

16. Defendants have declined to make any changes despite being alerted about the problems with the Website, and despite the fact that there are simple technical solutions available. Defendants could address most, if not all, of the legal deficiencies alleged in this action simply by adopting strict user registration and access controls on the SCRA Website. Other federal agencies, including the Social Security Administration and the Department of Homeland Security, have adopted such measures when operating analogous online verification systems. DoD has not.

17. VVA, VVA NYSC, and Chapter 77 therefore bring this action on behalf of their members in order to ask this Court to compel Defendants to properly secure veterans' Private Information. Mr. Barden seeks the same relief and also asks the Court to order DoD to pay the out-of-pocket costs he has suffered as a result of the scam perpetrated against him.

18. VVA's founding principle is "Never again will one generation of veterans abandon another." Through this action, Plaintiffs seek to ensure that no servicemembers or veterans will be targeted using sensitive information that the government has a duty to protect.

JURISDICTION AND VENUE

19. This action arises under, and alleges violations of, the Administrative Procedure Act ("APA"), 5 U.S.C. §§ 701-706, the Privacy Act of 1974, 5 U.S.C. § 552a, and the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552.

20. This Court has jurisdiction over this action under 28 U.S.C. § 1331 (federal question), 5 U.S.C. §§ 702, 704 (APA jurisdiction to review agency action), 5 U.S.C. § 552a(g)(1) (Privacy Act), and 5 U.S.C. § 552(a)(4)(B) (FOIA).

21. The requested relief is proper under 5 U.S.C. § 706 (APA relief), 5 U.S.C. § 552a(g)(1)(D) (damages), 5 U.S.C. § 552(a)(4)(B) (FOIA relief); 28 U.S.C. § 2201 (declaratory relief), 28 U.S.C. § 2202 (injunctive relief), and 28 U.S.C. § 2412, 5 U.S.C. § 552a(g)(4)(B) & 5 U.S.C. § 552(a)(4)(E) (costs and attorney's fees)

22. Venue lies in this district pursuant to 28 U.S.C. § 1391(e)(1)(c), 5 U.S.C. § 552a(g)(5), and 5 U.S.C. § 552(a)(4)(B), because Plaintiff Thomas Barden resides in Erie County; Plaintiff Chapter 77 has its principal place of business in Tonawanda, NY; and Plaintiffs VVA, VVA NYSC, and Chapter 77 each have at least one affected member who resides in the district. No real property is involved in this action. The Defendants are agencies or officers of the United States sued in their official capacities.

PARTIES

Plaintiffs

23. Founded in 1978, VVA is the only national veterans organization congressionally chartered and dedicated to the needs of veterans from the Vietnam era and their families. VVA is a membership-based organization with members from all branches of the military including the

Army, Navy, Air Force, Marine Corps, and Coast Guard. VVA is a nonprofit corporation organized under the laws of New York and headquartered in Maryland.

24. VVA has a longstanding commitment to defending veterans' privacy rights, one part of its core mission to foster, encourage, and promote the improvement of the condition of veterans. For instance, in 2006, VVA filed a class action lawsuit against the Department of Veterans Affairs ("VA"), after the VA lost millions of veterans' personal records, exposing them to risks of identity theft and fraud. That lawsuit, like this one, alleged violations of the Privacy Act.

25. VVA brings this action on behalf of its members. VVA's membership includes veterans whose Private Information is accessible through the SCRA Website.

26. VVA New York State Council is an organization that represents the members of all 36 VVA chapters in New York State, as well as VVA members-at-large in the State. VVA NYSC is organized under the laws of the State of New York. VVA NYSC brings this action on behalf of its membership, which includes veterans whose Private Information is accessible through the SCRA Website.

27. Chapter 77 is one of many local chapters affiliated with VVA organized to provide for the needs of veterans and their families. Chapter 77 was established in 1979, beginning as the Vietnam Veterans Outreach Center in the City of Buffalo, New York. In 1984, Chapter 77 was incorporated as a non-profit veteran's organization under the laws of New York. Its offices are located in Tonawanda, New York. Chapter 77 brings this action on behalf of its membership, which includes veterans whose Private Information is accessible through the SCRA Website.

28. Thomas Barden is a veteran of the Air Force. He retired at the rank of Master Sergeant after more than 20 years of service. Mr. Barden served in Vietnam, where he suffered injuries in a rocket attack. Later in his career, he oversaw maintenance of highly sophisticated surveillance aircraft as a senior non-commissioned officer. In that capacity, he was entrusted with high-level security clearances. Mr. Barden's Private Information is accessible through the SCRA Website.

29. Mr. Barden was the victim of an impostor scam that relied on private details about his military service that are accessible through the SCRA Website. The scam cost Mr. Barden hundreds of dollars as well as his computer, which was irreparably infected with malware. Like other veterans whose information is exposed through the SCRA Website, Mr. Barden suffers fear, stress, and considerable anxiety that he will (again) be targeted for scams or frauds because his Private Information is freely accessible on the SCRA Website. Mr. Barden is part of the membership of VVA, VVA NYSC, and Chapter 77.

Defendants

30. The Department of Defense is an agency of the federal government that oversees all military operations and personnel. DoD has responsibility for maintaining and safeguarding servicemembers' and veterans' military records. DoD operates the SCRA Website. DoD has authority to make, change, and enforce the rules and procedures governing disclosure of the Private Information and access to such information through the SCRA Website.

31. Jim Mattis is Secretary of Defense. He has ultimate authority to direct and control all DoD operations. This includes the authority to make, change, and enforce the rules and procedures governing disclosure of Private Information and access to such information through the SCRA Website. He likewise has authority to direct subordinates within DoD to take all

appropriate measures to bring the SCRA Website and DoD's disclosure practices into compliance with law. Secretary Mattis is sued in his official capacity.

32. Dana W. White is the Assistant to the Secretary of Defense for Public Affairs (ATSD-PA). According to an official Privacy and Security Notice posted on the SCRA Website, the Office of the Assistant Secretary of Defense-Public Affairs, which is the direct predecessor to the current ATSD-PA, is responsible for providing the SCRA Website, along with the Defense Manpower Data Center. Assistant Secrecy White is sued in her official capacity.

33. Anthony M. Kurta is currently performing the duties of Under Secretary of Defense for Personnel and Readiness ("USD(P&R)"). USD(P&R) is part of DoD and has primary responsibility for personnel management. The USD(P&R) oversees the Defense Manpower Data Center, which operates the SCRA Website. The USD(P&R) has authority to make, change, and enforce the rules and procedures governing disclosure of Private Information and access to such information through the SCRA Website. The USD(P&R) likewise has authority to direct subordinates within DoD to take all appropriate measures to bring the SCRA Website and DoD's disclosure practices into compliance with law. Acting Under Secretary Kurta is sued in his official capacity.

34. William H. Booth is Director of the Defense Human Resources Activity ("DHRA"). DHRA is a component of DoD with primary responsibility for providing and overseeing personnel data management operations for the entire Department. The Director of DHRA reports to the USD(P&R) and oversees DMDC, which operates the SCRA Website. The Director of DHRA has authority to make, change, and enforce the rules and procedures governing disclosure of Private Information and access to such information through the SCRA Website. The Director likewise has authority to direct subordinates within DoD to take all

appropriate measures to bring the SCRA Website and DoD's disclosure practices into compliance with law. Director Booth is sued in his official capacity.

35. Michael V. Sorrento, is Director of the Defense Manpower Data Center ("DMDC"). DMDC is a component of DoD with primary responsibility for providing information on personnel during and after their affiliation with DoD. DMDC is the central repository for DoD human resources information, both current and historic. DMDC manages the Defense Enrollment Eligibility Reporting System ("DEERS"), a DoD database from which the information on the SCRA Website is drawn. DMDC operates and controls the SCRA Website. Mr. Sorrento, as Director of DMDC, has the authority to make, change, and enforce rules and procedures governing disclosure of Private Information and access to such information through the SCRA Website. Mr. Sorrento also has authority to direct others within DMDC to take appropriate measures to bring the SCRA Website into compliance with law. Mr. Sorrento is sued in his official capacity.

36. The United States is sued under 5 U.S.C. § 552a(g)(1)(D) and 5 U.S.C. § 702 for actions of the Department of Defense and its agents.

LEGAL FRAMEWORK

37. The Privacy Act of 1974, 5 U.S.C. § 552a, regulates how the federal government may collect, maintain, use, and — most relevant here — disseminate personal information about citizens and permanent residents. The law imposes strict limits on how and when federal agencies may share personal information with third parties.

38. The Privacy Act protects essentially all personally-identifiable information that is contained in a federal database. More precisely, the Privacy Act protects any "record" that is contained in a federal "system of records." A "record" means any "item, collection, or grouping

of information about an individual" that contains the individual's "name, or the identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(4). A "system of records" is defined broadly to include "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).

39. The Private Information that Defendants make accessible through the SCRA Website qualifies as a "record" within a "system of records" subject to the Privacy Act.

40. The Privacy Act provides several important protections, three of which are relevant here.

Prohibited disclosure to third parties

41. *First*, the Privacy Act generally prohibits agencies from disclosing any records in a government database to any person (or to another agency) except with the prior, written consent of the individual to whom the record pertains. 5 U.S.C. § 552a(b) The Act contains 12 enumerated exceptions to this general rule, each of which permits disclosure to particular people or entities for specified uses.

42. Only one of these exceptions is relevant here. A record may be disclosed by an agency for a "routine use." § 552a(b)(3). All routine uses must be defined and published in the Federal Register by the agency that maintains the system of records. § 552a(e)(4)(D). Agencies must provide at least 30 days advance notice of any proposed routine use in order to provide an opportunity for public comment. § 552a(e)(11).

43. The published description of the routine use must "includ[e] the categories of users and the purpose of such use." § 552a(e)(4)(D). A valid routine use may only permit

disclosure of a record "for a purpose that is compatible with the purpose for which it was collected." § 552a(a)(7).

Administrative and technical safeguards and security measures

44. *Second*, the Privacy Act requires agencies to establish appropriate safeguards to protect records. Specifically, agencies must establish "administrative, technical, and physical safeguards to insure the security and confidentiality of records and 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." 5 U.S.C. § 552a(e)(10).

Accounting of disclosures

45. *Third*, the Privacy Act requires agencies to keep an accounting of their disclosures of records, including each and every disclosure made pursuant to a routine use. § 552a(c)

46. Specifically, the Act requires the agency to keep an accurate accounting of the name and address of the person (or agency) to whom each such disclosure is made, as well as the date, nature, and purpose of each such disclosure. § 552a(c)(1)(A)-(B).

47. The agency must retain this accounting for the life of the underlying record or for five years, whichever is longer. § 552a(c)(2). Individuals are entitled to obtain a copy of this accounting in order to learn who has obtained information pertaining to them. § 552a(c)(3).

* * *

48. As alleged herein, the SCRA Website flagrantly violates all of these requirements. Defendants, through the SCRA Website, are disclosing veterans' private records to anyone for any purpose. They have not implemented any meaningful access controls or other administrative

or technical safeguards. They have also failed to properly keep track of who obtains records through the Website and for what purpose.

FACTS

Scammers targeted Plaintiff Thomas Barden using details accessible on the SCRA Website.

49. Plaintiff Thomas Barden was victimized by scammers using personal details accessible on the SCRA Website.

50. On or about March 2016, Mr. Barden received a phone call from a person who identified himself as a Microsoft-affiliated representative.

51. The caller knew various personal details about Mr. Barden. Specifically, during the course of the conversation, the caller demonstrated that he knew Mr. Barden's name, date of birth, full address, and telephone number.

52. In addition, the caller was armed with details about Mr. Barden's military service. In particular, the caller mentioned the specific month and date that Mr. Barden left the armed forces, and also mentioned that Mr. Barden had served in the Air Force. These details precisely match information that Defendants make available in response to searches on the SCRA Website.

53. Mr. Barden had not provided any of this personal information to the caller.

54. Upon information and belief, the personal details that the caller had regarding Mr. Barden's military service were improperly disclosed by Defendants through the SCRA Website. Those details are easily accessible through the SCRA Website by running a search using Mr. Barden's name and birthdate, which the caller had.

55. Mr. Barden regarded the personal details about his service as the type of information that would only be available to a company that had some official, authorized relationship with him or with the government.

56. Mr. Barden was persuaded that the caller was legitimate because the caller had access to these personal details.

57. After he had gained Mr. Barden's trust, the caller, supposedly affiliated with Microsoft, asked Mr. Barden to grant him remote access to the computer in order to diagnose any problems. Mr. Barden agreed, giving the caller direct access to his computer through the internet. The caller examined various supposed problems with the computer, all the while still speaking with Mr. Barden on the phone. During the course of this supposed diagnostic examination, the caller told Mr. Barden that his computer lacked a "firewall" to protect against viruses and intrusions.

58. The caller persuaded Mr. Barden that his computer was at risk. Mr. Barden agreed to purchase firewall software to protect his computer. The caller, who still had remote access to the machine, facilitated the purchase by directing the computer to an online payment screen. The screen was pre-filled with Mr. Barden's name and address. Mr. Barden inputted his credit card details, purchased the software for $300, and installed it while still on the phone with the caller. The call ended soon thereafter.

59. At that point, Mr. Barden believed that he had purchased genuine security software from a legitimate company.

60. Approximately nine months later, on or about December 2016, Mr. Barden received a phone call from a person identifying himself as a representative of the same company that had provided the firewall. The caller told Mr. Barden that the company was going out of

business and, as a result, that it was going to refund the purchase price of the firewall. The caller asked for remote access to the computer. Mr. Barden, still persuaded that he was dealing with a legitimate business, again granted the caller remote access to his computer.

61. Using the remote access, the caller made a seemingly legitimate Microsoft screen appear. The screen had three options by which Mr. Barden could supposedly receive the refund: direct deposit to a bank account, PayPal, or Western Union. Mr. Barden indicated that he only used a bank account and, at the caller's request, provided the name of the bank.

62. Immediately after Mr. Barden provided the caller with the name of his bank, the caller directed the Barden's computer to that bank's website and asked Mr. Barden to log in.

63. Mr. Barden became very suspicious at this point. He believed that if he were to log in he would effectively give the caller unfettered access to the funds in his account. He refused to.

64. In response, the caller became hostile and dropped the pretense of being a representative of a legitimate company. The caller told Mr. Barden that he would be locked out of his computer and would lose access to all of his files unless he paid more money.

65. By this point, the caller had indeed locked Mr. Barden of the computer. The computer displayed an unfamiliar screen that required a password. Mr. Barden understood that the computer was locked and unuseable unless the caller remotely inputted the password to unlock it. The caller was, in effect, holding the computer for ransom.

66. Mr. Barden refused to pay. He hung up the phone, closed his computer, and unplugged his connection to the internet.

67. Some days later, Mr. Barden tried to log back into his computer, but he was unable to do so.

68. Now acutely aware that he had been targeted for a scam, Mr. Barden became very anxious about the privacy of the personal information to which the scammer had access.

69. Mr. Barden sought advice about what to do with his compromised computer. He was advised that the computer was irretrievably infected with the scammer's malware and that there was no way to repair the computer or recover his data. He was further advised that he should destroy the computer's hard drive in order to prevent the possibility of further intrusions, data theft, or spread of malware. Mr. Barden followed this advice, breaking the hard drive into pieces. Indeed, Mr. Barden was so shaken by the episode and so concerned about his privacy that he threw the pieces of the destroyed hard drive into multiple trash cans over several days in order to ensure that it could not be pieced back together.

70. Now left with no computer, Mr. Barden purchased a used laptop for $350 as a replacement.

71. Mr. Barden has continued to receive regular, harassing phone calls from people identifying themselves as representatives of the company from which he bought the firewall. Mr. Barden refuses to speak with them.

72. Mr. Barden suffered significant anxiety and stress as a result of this scam. The scammer's attack on his computer and violation of his privacy caused him significant emotional harm.

73. Mr. Barden became even more anxious when he learned about the SCRA Website and discovered that allows anyone to access his Private Information. He realized that the scammers may have used the website to obtain the details about his military service that they had deployed to gain his trust.

74. The fact that essentially anyone can access his personal information through the SCRA Website has caused Mr. Barden significant further anxiety and stress. He is particularly concerned that he could be targeted again by scammers, or that his private information could be misused in other ways.

75. As a result of the scam and the SCRA Website, Mr. Barden has become cautious and distrustful, particularly with respect to his telephone communications, electronic devices, and online life. He now limits his activities in various ways. For instance, he now uses his laptop or phone only for as short a time as possible. He does not use his own personal computer for sensitive online activities like banking. He deletes emails without reading if he does not quickly recognize the sender. He refuses to answer phone calls or text messages unless he recognizes the phone number.

76. Mr. Barden fears that he, along with millions of other veterans in the SCRA Website, remain easy targets for scams and frauds.

Mr. Barden's frustrated effort to learn who has obtained his private information.

77. Mr. Barden would like to understand how broadly his Private Information has been disclosed as a result of Defendants' failure to properly secure the SCRA Website. He also wishes to learn who, exactly, has obtained his Private Information.

78. On June 9, 2017, Mr. Barden, though counsel, submitted a formal request under the Freedom of Information Act and Privacy Act seeking disclosure of any and all accountings kept pursuant to 5 U.S.C. 552a(c), as well as any similar records that detail who has searched for and obtained his Private Information through the SCRA Website. The request was send to the Office of the Secretary of Defense and Joint Staff ("OSD/JS"), which oversees DMDC, and also to DMDC itself.

79. To date, neither OSD/JS or DMDC have provided any responsive records.

80. DMDC acknowledged receipt of the request in a letter dated June 16, 2017. The letter explained that DMDC could not proceed because the request had not included sufficient personally identifying information. In particular, the letter stated that Mr. Barden's place of birth was required in order to process the request.

81. The original request had included Mr. Barden's full name, date of birth, and SSN. Those details are more than sufficient for a member of the public to locate and obtain Mr. Barden's Private Information through the SCRA Website.

82. Mr. Barden, through counsel, provided DMDC with his place of birth.

83. In a letter dated June 23, 2017, DMDC acknowledged that it had received the requested detail on June 21, 2017. The letter further stated that DMDC had "considered and is unable to grant th[e] request in accordance with the Privacy Act . . . at this time." The letter explained that "additional research is required regarding your request for records from the Defense Manpower Data Center Servicemembers Civil Relief Act database (SCRA). The results will be provided as they become available."

84. DMDC has provided no estimate or other indication as to how long it will take to complete its research and provide a response. OSD/JS has indicated, for its part, that DMDC is solely responsible for responding to the request.

85. Mr. Barden remains in the dark about who has obtained his Private Information through the SCRA Website.

The SCRA Website creates an ongoing and imminent risk of frauds, scams, and identity theft.

86. The SCRA Website makes veterans, including Mr. Barden and other members of the Plaintiff organizations, easy targets for frauds and scams. By leaving details of their military

service easily accessible, Defendants are exacerbating and contributing to the heightened risk of being targeted that veterans face.

87. The Private Information can be used to perpetrate a variety of scams and frauds, including those generally fall under the rubric of "imposter scams" and "identity theft."

88. In an imposter scam, the perpetrator pretends to be someone who the target trusts in order to convince the target to send money or purchase a fraudulent product. According to consumer complaint data compiled by the Federal Trade Commission ("FTC") in 2016, the most common form of imposter scam involves the perpetrator impersonating a government official. In other common variants, the scammer presents himself as a representative of a legitimate, well-known business, or purports to be a legitimate tech support provider. Mr. Barden was a victim of this type of scam.

89. The SCRA Website facilitates imposter scams by allowing would-be scammers to easily obtain details about a person's military service. Veterans and servicemembers, including members of the Plaintiff organizations, do not realize that the Private Information available on the SCRA Website is accessible to anyone. Instead, they expect that such information is not ordinarily public and it is generally available only to government officials or other legitimate government-affiliated business or entities. As a result, scammers armed with the Private Information can use the information to secure veterans' confidence.

90. Another common type of fraud is known as identity theft. Identity theft describes a wide range of schemes in which the perpetrator appropriates the victim's personal identifying information to commit fraud or theft.

91. The SCRA Website facilitates identity theft in at least two ways.

92. First, the SCRA Website effectively encourages veterans to hand over their SSN to third-parties who ask for it in order to run searches on the Website. Because the SCRA Website is freely accessible to anyone, it has come to be used by third-parties as an all-purpose means to verify whether someone has served in the military, even though the only legitimate use of the website by third parties is to determine SCRA protection. Because Defendants permit (and, indeed, encourage) users to search using the SSN, they incentivize third-parties to require veterans to disclose their SSN for the purpose of querying the SCRA Website.

93. The risks from disclosing SSNs to third parties are well known. With access to a person's SSN it is a relatively simple matter for a bad actor to perpetrate all manner of scams such as obtaining fraudulent credit cards or fraudulent tax refunds in the victim's name.

94. By permitting anyone to query the SCRA Website using an SSN for any purpose, Defendants are leading veterans to disclose their SSNs to third parties. Those third parties may fail to properly protect the SSN leading to its fraudulent use by others, or they may themselves use the SSN improperly.

95. Second, the SCRA Website may allow scammers to obtain fraudulent credentials in another person's name. Online identity verification companies such as ID.me, SheerID, and GovX currently use the SCRA Website as one means to determine whether a person is a servicemember or a veteran. Such services issue a digital credential verifying veteran status that can be used on various third-party sites to get access to veteran-specific discounts and other benefits. As one means of verifying a person, these services ask users to provide identifying details including name and date of birth, and sometimes other identifying details including SSN. They use those details to run a search through the SCRA Website. If the SCRA Website returns a positive response, the service issues a digital credential.

96. Scammers can exploit these services' reliance on the SCRA Website in order to obtain fraudulent digital credentials. By providing a name and date of birth and other publicly-accessible information about another person, the scammer may be able to "verify" that person's identity and gain control of a fraudulent digital credential in that person's name.

The SCRA Website contributes to the high risk of fraud that veterans face.

97. Veterans and servicemembers, including members of the Plaintiff organizations, face a high risk of being victimized by scammers. The SCRA Website contributes to this risk.

98. Veterans and servicemembers are prime targets of scams for a variety of reasons. They often receive steady, guaranteed income from the government. They are accustomed to dealing frequently with government officials and bureaucracies that require disclosure of various private information. Servicemembers have been required to share their SSNs routinely while on duty. Many are therefore too willing to share the SSN even after they leave the service. Servicemembers and veterans also often feel special affinity and goodwill for one another and for organizations associated with the military; scammers can exploit this goodwill to gain their trust. Many veterans also suffer from injuries, including Post-Traumatic Stress, that make them particularly vulnerable to manipulation by con artists.

99. The Federal Trade Commission has documented the high risk that veterans and servicemembers face. Through its Consumer Sentinel Network ("CSN"), the FTC compiles voluminous data about consumer complaints that Americans have reported to federal and state agencies and various private organizations. Each year CSN publishes a "data book" analyzing and summarizing the prior year's complaints. The CSN data book separately analyzes complaints filed by veterans and servicemembers, providing an annual snapshot of the nature and extent of the threat veterans face.

100. The CSN data reveal that the number of veterans and servicemembers affected is growing every year. In 2014, the CSN compiled 98,087 complaints from people affiliated with the military, including at least 58,175 from veterans. By 2016, those numbers had grown to 115,984 total military complaints including at least 69,801 from veterans. This increase reflects a long-term trend, with complaints rising year-on-year since at least 2012.

101. Among all military-affiliated consumers, the vast majority of reported complaints involve veterans rather than individuals currently in service.

102. Impostor frauds and identity theft — exactly the kinds of frauds that the SCRA Website facilitates — are the largest threats that veterans and servicemembers face, according to the CSN data. In 2016, impostor scams comprised 32% of reported complaints from military consumers (including veterans); identity theft comprised 30% of such complaints. No other type of complaint registered even in the single digits.

103. Impostor scams have proliferated at an alarming pace. In 2012, only 4,477 impostors scams were reported by military consumers (including veterans), comprising only 7% of their complaints. In 2016, the number of such complaints spiked to 37,275, comprising 32% of military complaints. Impostor scams are now the most common type of fraud that veterans face, outpacing even identity theft.

104. Veterans are disproportionately targeted for impostor frauds and identity theft. Among the general population, impostor scams and identity theft each comprise only 13% of complaints, while among veterans and other military-affiliated individuals, these types of frauds each constitute upwards of 30% of reported complaints.

105. Veterans, including Mr. Barden and other members of the Plaintiff organizations, suffer considerable anxiety, stress, and other emotional and psychological harms as a result of

Defendants' failure to properly protect their Private Information and the risk of fraud, scams, and identity theft they thereby create.

106. Other components of the government recognize that veterans face a concrete risk of identity theft and other scams. The VA, for example, has taken a number of steps to attempt to mitigate the problem. It has launched a program named More Than a Number that is meant to spread awareness of identity theft and encourage preventive measures. The VA operates an Identity Theft Help Line for veterans who know or suspect that they have been targeted. The VA has also launched a website that offers veterans a variety of resources and information about the problem.

107. DoD itself acknowledges the risk that servicemembers and veterans face. For instance, official DoD policy established in 2012 recognizes that "the threat of identity theft has rendered th[e] widespread use of [Social Security Numbers] unacceptable." DoD Instruction 1000.30, Enclosure 2, ¶ 1(a). DoD has taken steps to limit or eliminate the use of SSNs in other areas of its operations. In many instances, DoD has instituted the use of non-sensitive DoD-specific identification numbers in place of the SSN.

108. Nevertheless, Defendants continue to permit anyone to query the SCRA Website using an SSN for any purpose.

109. Despite the real and imminent danger of scams and frauds faced by veterans, including Plaintiffs and their members, Defendants have failed to take any measures to limit who can use the SCRA Website and for what purpose. They have also failed to take sufficient measures to eliminate the need for veterans and servicemembers to turn over their SSN to third parties who use the SCRA Website.

Veterans suffer privacy harms when they cannot control who learns details about their service.

110. Veterans, including Mr. Barden and other members of the Plaintiff organizations, have a strong privacy interest in controlling who learns details about their service. They have often been subject to discrimination or disparate treatment on account of their service. By allowing open access to the SCRA Website, Defendants prevent such veterans them from being able to decide who learns details about their service.

111. The sensitive details disclosed by Defendants include the fact that an individual has served; that an individual served during during a particular conflict or era; the component of the military in which an individual served, including whether he or she was called up to active duty out of the Reserves or National Guard; and whether an individual has been notified of a future call-up to active duty.

112. Disclosure of these details exposes veterans and servicemembers to concrete privacy harms, including social stigma, workplace discrimination, and similar prejudice in other areas of life.

113. Veterans who serve in armed conflicts, including Mr. Barden and other members of the Plaintiff organization, have often faced stigma or prejudice after leaving the service. Upon their return, they often have to contend with negative prejudices regarding their skills, abilities, mental or physical health, and other personal characteristics. Veterans who served in Vietnam have suffered particularly acute social stigma on account of their service. They have faced public condemnation, personal rebukes, and abuse from fellow citizens, in addition to general disrespect and suspicion on account of their service in that conflict.

114. The stigma and prejudice against veterans is manifest in many domains. For example, employers are often reluctant to hire veterans; indeed, veterans face markedly higher

rates of unemployment. The reasons for such discrimination include, for example, preconceptions regarding veterans' mental health or physical health; reluctance to accommodate service-related disabilities; and misconceptions regarding the skills (or lack thereof) possessed by veterans who have frequently delayed or foregone higher education and other traditional career paths in order to serve. These forms of prejudice were particularly acute with respect to veterans from the Vietnam era.

115. Reservists and members of the National Guard face similar difficulties. Employers are often reluctant to hire because they are concerned that the individual will miss work for ongoing training obligations or if called up to active duty.

116. The government itself has recognized that veterans (and Reservists and Guardsmen) face this kind of prejudice, enacting laws and regulations prohibiting certain limited forms of discrimination.

117. Because they often face these various forms of stigma, prejudice, and discrimination, veterans and servicemembers have a strong interest in being able to decide for themselves whether to share information about their military service.

118. Members of the Plaintiff organizations, including Mr. Barden, have often carefully limited who they tell about where they served, when they served, how long they served, and what component of the military they served in. They often disclose details about their service history only to families, friends, and fellow veterans.

119. By allowing essentially unfettered access to information about veterans' military service through the SCRA Website, Defendants have taken the decision whether to share such information out of the hands of veterans, including Mr. Barden and other members of the Plaintiff organizations.

120. The SCRA Website exposes veterans and servicemembers to other concrete privacy harms as well. For instance, by disclosing information about precisely when reservists and guardsmen have been called up to future active duty, the Website may allow a criminal to learn when they are likely to be absent from their homes. This may expose their household and family members to criminal predation.

121. Defendants have also left the SCRA Website open to be mined by private data brokers. Data brokers are private companies whose business is to collect and maintain data on private citizens for the purpose of analyzing, packaging, and selling that information for profit. Because the SCRA Website is wide open for anybody to use for any purpose, data brokers can easily obtain Private Information about servicemembers and veterans (including members of the Plaintiff organizations) without their consent, and add it to the ever-larger and more intrusive databases of personal information that these companies analyze and sell for profit.

The rules that govern disclosure through the SCRA Website permit anonymous, essentially unfettered access to Private Information by anyone for any purpose.

122. The SCRA Website contains information about virtually everyone who has served on active duty in the armed forces at any time since September 30, 1985, amounting to millions of individuals. Defendants have configured the Website so as to make all of their Private Information available to anyone, anonymously, for any purpose.

123. The SCRA Website does not require a user to provide written consent from a servicemember to request information.

124. In order to search for one record at a time, anybody can simply direct their web browser to the SCRA Website and input (1) last name and DOB or (2) last name and SSN of the veteran or servicemember whose records are sought. In addition, the user must input an "active

duty status date" that falls anywhere within the veteran or servicemembers' dates of active service, within 367 days after the end of active service, or after notification of a future call up to active service.

125. If the name and birthdate (or name and SSN) match a record in the database — and if the active duty status date that was entered falls within range — then the system produces a PDF certificate that provides all of the Private Information described above. The certificate is returned within a matter of seconds.

126. The requirement to input an active duty status date is no obstacle for a user who wishes to obtain a veteran or servicemember's Private Information through the Website, even if the user does not know in advance when the person served in the military. A user can simply run multiple searches, entering arbitrary active duty status dates spaced one year apart until the system returns a hit.

127. Defendants do not require a user to provide any information about themselves at all about in order to search for and obtain a single record through the SCRA Website. Defendants do not even ask the user why or for what purpose he or she is seeking disclosure. Indeed, the User Manual to the SCRA Website includes a list of Frequently Asked Questions including "Does the website restrict my access in any way?" The manual states in response that for requests for a single record "there are no restrictions. Anyone can request information about an individual, at any time."

128. The SCRA Website also allows anyone to request enormous numbers of records at once using a process the DMDC describes in the User Manual as a "multiple record request."

129. Using a multiple record request, a user can submit up to 250,000 requests at a time by uploading a text file to the SCRA Website that contains the search terms for each individual request — *i.e.* name, birthdate and/or SSN, and active duty status date(s).

130. A user can submit up to 50 such multiple record requests in a 24-hour period. A single user can thus run up to 12.5 million unique requests per day.

131. The SCRA Website typically delivers responses to multiple record requests within 24 hours after the search file is uploaded. Responses are provided in the form of a spreadsheet.

132. To conduct a multiple record request, a user must create an account on the SCRA Website. But to create an account, all a user must do is choose a username and password and input a "company name."

133. Defendants do not ask for any other identifying information in order to create an account. They do not ask for a name, address, proof of identity, email address, or any other contact information. The do not inquire about the purpose for which the SCRA Website is being used. And while they ask for a company name, they do nothing to verify that the company name is legitimate, nor do they ask for any information (such as an Employer Identification Number or mailing address), that might permit the government to identify the company.

134. Defendants do not keep track of the identity of those to whom they disclose Private Information through the SCRA Website. According to the Privacy and Security Notice that accompanies the SCRA Website, DoD does not make any attempts "to identify individual users or their usage habits" aside from routine monitoring of network traffic on the site (e.g. presumably collecting IP address) for site security/statistical purposes, or if there are an "authorized law enforcement investigations." The SCRA User Manual similarly states that when a record is requested, DMDC only retains the search queries along with the IP address of the

requester, a timestamp, a unique Report ID number, and, with respect to multiple-record requests, the username.

135. While the Website does not require a user to input an SSN in order to run a single- or multiple-record search, Defendants nevertheless encourage users to obtain and use the SSN. The SCRA Website User Guide states, "To improve the quality of the match results, DMDC recommends that you enter as much known information as possible." When a single-record search is conducted using only a name and birthdate, the resulting certificate states prominently: "WITHOUT A SOCIAL SECURITY NUMBER, THE DEPARTMENT OF DEFENSE MANPOWER DATA CENTER CANNOT AUTHORITATIVELY ASSERT THAT THIS IS THE SAME INDIVIDUAL THAT YOUR QUERY REFERS TO. NAME AND DATE OF BIRTH ALONE DO NOT UNIQUELY IDENTIFY AN INDIVIDUAL." Similarly, the spreadsheet that is returned to users in response to a multiple-record request provides a "match result code" that scores the quality of the match. Those codes range from "1" (the highest quality result) indicating that the system matched SSN, first and last name, as well as DOB, all the way down to "6" (the lowest quality result), which means that only a name and date of birth matched.

136. In these ways, Defendants actively encourage users of the Website to demand that veterans and servicemembers turn over their SSNs for purposes of running a query.

Defendants are disclosing veterans' private information beyond any legitimate use.

137. The legitimate purpose of the SCRA Website is to provide a straightforward way to determine whether a person is protected by the Servicemembers Civil Relief Act, which offers various legal and consumer protections to individual who are (or recently were) on active duty. But the website permits access to anyone for any purpose, far beyond any legitimate SCRA use.

138. The information that is accessible through the SCRA Website is drawn from a much larger system of records operated by Defendants known as the Defense Eligibility and Enrollment Reporting System ("DEERS").

139. DEERS is a massive personnel and human resources database maintained by Defendants for the purpose of determining eligibility for benefits, for issuing DoD badges and identification cards, and for other similar purposes.

140. DoD has issued a System of Records Notice ("SORN") for DEERS, the most recent version of which was published in the Federal Register on July 27, 2016. 81 Fed. Reg. 49,210.

141. The DEERS SORN specifies 32 routine uses for records contained in the database.

142. None of the routine uses in the DEERS SORN authorizes disclosure for purposes of verifying eligibility for SCRA protection.

143. DoD has issued a separate document, styled as a "Privacy Act Statement / Privacy and Security Notice" specifically for the SCRA Website and available for download on the website itself (hereinafter, "SCRA Website Privacy Act Statement"). The SCRA Website Private Act Statement was never published in the Federal Register.

144. The SCRA Website Privacy Act Statement purports to describe the following routine use for the Website: "To obtain an individual's active duty status on a given date, in order to determine if they are eligible for protection under the Servicemembers Civil Relief Act."

145. Defendants have failed to implement any limits on third parties' access to the SCRA Website that would restrict its use to determining eligibility for SCRA protection.

Defendants have been alerted of the problems with the SCRA Website but have declined to adopt the simple measures required to come into compliance.

146. Defendants have repeatedly been alerted about the privacy concerns with the SCRA Website. They have declined to take any steps to change how the Website operates or the disclosure rules that it implements.

147. Senator Richard Blumenthal of Connecticut submitted a letter, dated July 24, 2014, to the then-Director of DMDC expressing concern about potential misuse of the SCRA Website. Senator Blumenthal expressed particular concern that commercial enterprises may have inappropriate access to the SCRA Website. Senator Blumenthal asked DMDC to explain whether "it [is] within the bounds of the website's terms of use for a for-profit entity to use this website on a bulk and regular basis to verify a customer's military status." Senator Blumenthal further asked whether DMDC had observed "any suspicious activity" on the Website and directed DMDC to provide "information regarding what steps DMDC has taken to ensure that this website is not being used inappropriately."

148. In response to Senator Blumenthal's letter, DMDC admitted that it "does not consider for-profit companies extracting data for other uses within the bounds of the terms of the website, such as for-profit entities offering discounts to their products or services for Service members."

149. Despite acknowledging that such uses are improper, DMDC's letter went on to admit that "the information is freely available on the DMDC's SCRA website." In fact, DMDC squarely acknowledged that "the SCRA website is a public website (*i.e.* available to anyone with access to the internet)" even while admitting that "the information contained within it is sensitive in nature."

150. DMDC's response to Senator Blumenthal, dated October 6, 2014, described no measures to screen out improper uses or to restrict access only to those using the website for legitimate SCRA purposes. Indeed, no such measures exist. DMDC's letter did purport to describe "several layers of protection of sensitive information." But the only "protection" DMDC describes is the requirement that a user must input a name and date of birth (or SSN) in order to run a search. Of course, that is no protection at all and does not limit access only for authorized purposes. Anybody can input those search terms for any reason.

151. Finally, DMDC acknowledged in its response to Senator Blumenthal that it does not monitor whether the website is being used for such improper purposes. DMDC stated that it "only monitor[s] the amount of traffic and destinations" and that "[i]nternal DMDC and DoD-level monitoring tools alert us to unusual amounts of traffic to or from unexpected locations, *e.g.* overseas or unfriendly nations."

152. The following year, Defendants were again alerted about the privacy concerns with the SCRA Website. Attorney John J. Deschauer, Jr., of the Squire Patton Boggs law firm sent a detailed memorandum, dated July 29, 2015, to the General Counsel of Defense Human Resources Activity, a component of DoD that oversees DMDC and the SCRA Website. The memo recounted in great detail the problems with DoD's current rules permitting unfettered access to the SCRA Website. The memo described the privacy risks and harms that the website created. It also discussed in detail DoD's legal obligations under the Privacy Act. The memo included 19 supporting exhibits documenting its claims.

153. The General Counsel of the DHRA responded to Mr. Deschauer's memorandum by email dated October 26, 2015. The email acknowledged receipt of the memorandum, but failed to engage with the legal and policy concerns identified therein. Instead, the email simply

asserted, without any explanation or support, that "The release of information from the SCRA Website is consistent with DoD policy regarding the disclosure of information about service members."

154. Defendants have failed to make any substantive changes to the SCRA Website despite these repeated efforts to alert them about their legal obligations and the privacy harms that they are inflicting on veterans and servicemembers.

155. DoD's failure to take any action is particularly remarkable given that the problems can easily be addressed. As Mr. Deschauer's letter suggested, DoD could address its obligations under the Privacy Act simply by imposing security measures that better control who accesses the SCRA Website and for what purpose.

156. Other agencies of government that operate similar verification services have implemented just this type of solution. For example, the Social Security Administration ("SSA") operates a service for employers to verify whether a SSN matches a particular name. In order to use the service, users must apply for an account. To obtain an account users must provide the following pieces information, which allow SSA to identify them and verify that they have a legitimate reason to use the service: (1) type of employer/employee; (2) company EIN; (3) company or business name; (4) company phone number; (5) indication if you are a third-party submitter registering to do business on behalf of another company; (6) name as it appears on your Social Security card; (7) SSN; (8) DOB; (9) preferred mailing address; (10) work phone number; (11) fax number (optional); (11) e-mail address; and (12) answers to five security questions. If an account is approved by SSA, users must use their credentials to log in every time they wish to use the service. Moreover, each time a user logs in, he or she must accept the terms of a user certification statement.

157. The Department of Homeland Security ("DHS") has similar registration and verification requirements for third-parties who wish to use its E-Verify system, which is meant to allow employers to determine whether an individual has work authorization. As with the SSA system, users of E-Verify must apply for an account by providing multiple pieces of verifiable identifying information. They are also required to agree to a Memorandum of Understanding that specifies the circumstances in which users are allowed to query the system.

158. Defendants have not implemented any similar controls on the SCRA Website.

CAUSES OF ACTION

FIRST CLAIM FOR RELIEF
Violation of Administrative Procedure Act
(Unlawful disclosure and inadequate safeguards under the Privacy Act)

159. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

160. The APA provides for judicial review of agency actions causing legal harm or adverse effects to a plaintiff. 5 U.S.C. § 702. The APA requires the Court to deem unlawful and set aside agency actions, findings, and conclusions that are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). The APA also requires the Court to compel agency action that has been unlawfully withheld or unreasonably delayed. 5 U.S.C. § 706(1).

161. Defendants have taken final agency action by adopting and implementing rules and procedures that govern the disclosure of Private Information through the SCRA Website. Those rules and procedures are described in the SCRA Website User Guide, the SCRA Website Privacy Act Statement, and other official statements of Defendants and their agents or

employees. The final agency action in is also embodied and evidenced by the operation of the SCRA Website itself.

162. Under Defendants' disclosure rules and procedures, adopted and implemented through the SCRA Website, anyone can obtain Private Information — including that of Plaintiff Barden and members of VVA, VVA NYSC, and Chapter 77 — by running a simple search on the SCRA Website for any reason. Defendants' rules and procedures allow anyone to conduct a search on the SCRA Website and obtain the Private Information for any purpose.

163. This agency action is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" within the meaning of the APA because it violates the Privacy Act, 5 U.S.C. § 552a.

164. In particular, Defendants' actions violate the Privacy Act's requirement that an individual's records contained in a government system of records may not be disclosed to any third party without the individual's express written consent, unless for a permitted use specifically enumerated in the Act. 5 U.S.C. § 552a(b).

165. The Privacy Act permits defendants to establish "routine uses" of information, which operate as one kind of exception to the Act's general prohibition on disclosure. 5 U.S.C. § 552a(b)(3). In order to be valid, a routine use must be published in the Federal Register and must describe "the categories of users and and the purpose of such use," among other requirements. 5 U.S.C. § 552a(e)(4)(D).

166. Defendants have issued the SCRA Website Privacy Act Statement, which describes the a single purported routine use: "[t]o obtain an individual's active duty status on a given date, in order to determine if they are eligible for protection under the Servicemembers Civil Relief Act."

167. This purported routine use is invalid, unlawful, and of no effect for two reasons: it was not published in the Federal Register and it fails to specify the "categories of users" to whom disclosure is permitted. This purported routine use therefore cannot serve as an exception to the Privacy Act's general prohibition on disclosure.

168. The Private Information accessible through the SCRA Website is drawn from DEERS, which is a system of records within the meaning of the Privacy Act. DoD has published a System of Records Notice in the Federal Register that specifies all permitted routine uses of information in DEERS. 89 Fed. Reg. 49,210. None of those routine uses address or encompass disclosure through the SCRA Website.

169. Defendants' rules and procedures for disclosure of the Private Information through the SCRA Website allow disclosure far beyond any duly-established routine use, any purported routine use, or any other exception under the Privacy Act. Defendants allow disclosure through the SCRA Website to anyone, for any purpose, at any time. Defendants have failed to implement any measures to ensure that disclosures are only made for authorized uses or to prevent disclosure for unauthorized uses. These actions and failures to act violate the Privacy Act's prohibition on unauthorized disclosure. 5 U.S.C. § 552a(b).

170. Defendants actions and failures to act also violate § 552a(e)(10) of the Privacy Act, which requires Defendants to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records."

171. Defendants have failed to implement any technical or administrative safeguards to prevent unauthorized disclosure of the Private Information. Indeed, Defendants' have admitted that their rules and procedures governing the SCRA Website do not include any measures to ensure that records are disclosed only to authorized people for authorized purposes.

172. Defendants' actions have had adverse effects on members of the Plaintiff organizations including Mr. Barden. Among other harms, Mr. Barden has suffered direct out-of-pocket costs as a result of a scam that relied on the use of personal details that Defendants have made freely available through the SCRA Website. Members of VVA, VVA NYSC, Chapter 77, and Plaintiff Barden suffer anxiety, stress and other emotional and psychological harm because Defendants make their Private Information freely available. They are harmed by the risk of identity theft, impostor frauds, and other scams that Defendants actions directly create. They suffer a variety of privacy harms because Defendants' actions prevent them from controlling who may learn their Private Information. They also suffer harm because they are deprived of substantive and procedural rights guaranteed to them by the Privacy Act.

173. Plaintiffs are entitled to judicial review because they have suffered legal wrongs, have been adversely affected, and remain aggrieved by Defendants' final actions. Plaintiffs have no other adequate remedy for these violations. So long as Defendants' unlawful rules and procedures governing the SCRA Website remain unchanged, Mr. Barden and members of the Plaintiff organizations will continue to suffer harm.

SECOND CLAIM FOR RELIEF
Violation of Administrative Procedure Act
(Failure to keep an accounting of disclosures required by the Privacy Act)

174. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

175. The Privacy Act, 5 U.S.C. § 552a(c)(1)(A)-(B), requires Defendants to keep an accurate record of the date, nature, and purpose of each disclosure of a record, as well as the name and address of the person to whom the disclosure is made. The Act requires Defendants to retain such accountings for five years or the life of the record, whichever is longer. § 552a(c)(2).

176. Defendants' rules and procedures governing the SCRA Website violate these provisions of the Privacy Act because they do require Defendants to obtain or record the name and address of users who search for and obtain Private Information through the SCRA Website. They also do not require Defendants to ascertain or record the nature and purpose of each disclosure of a record. Defendants therefore cannot and do not maintain a proper accounting of disclosures as required by the Privacy Act.

177. Defendants' action or failure to act in this regard is final agency action and is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" within the meaning of the APA, 5 U.S.C. § 706(2)(A), because it squarely violates the Privacy Act, 5 U.S.C. § 552a(c)(2). Defendants have likewise "unlawfully withheld" action required by law. 5 U.S.C. § 706(1).

178. Members of VVA, VVA NYSC, Chapter 77, and Plaintiff Barden suffer legal wrongs and are adversely affected by Defendants' action or failure to act in this regard because without a proper accounting of disclosures they are unable to ascertain who has accessed their Private Information or whether their Private Information has been accessed improperly. They are unable to take appropriate precautions in the event that Defendants have disclosed their Private Information to individuals or entities who will misuse it. If they are victimized using information accessible through the SCRA Website, as Mr. Barden was, they are unable to determine the identifying information of the person or entity who may have been responsible. In addition, they are deprived of substantive and procedural rights guaranteed by the Privacy Act.

179. Plaintiffs are entitled to judicial review because they have suffered legal wrongs, have been adversely affected, and remain aggrieved as a result of Defendants' final actions or failure to act. Plaintiffs have no other adequate remedy for these violations. So long as

Defendants' continue to fail to keep a proper accounting of disclosures through the SCRA Website remain, Mr. Barden and members of the Plaintiff organizations will continue to suffer harm.

THIRD CLAIM FOR RELIEF
Violation of Privacy Act
(Compensation for actual damages suffered by Plaintiff Barden)

180. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

181. Defendants have violated Plaintiff Barden's rights under the Privacy Act by disclosing his Private Information through the SCRA Website without his consent and without any other lawful purpose, in violation of 5 U.S.C. § 552a(b); by failing to comply with the Privacy Act's requirement to implement safeguards to protect the security and confidentiality of his records accessible through the SCRA Website, as required by 5 U.S.C. § 552a(e)(10); and by failing to keep an accounting of disclosures of his Private Information through the SCRA Website as required by 5 U.S.C. § 552a(c).

182. In committing these violations of the Privacy Act, Defendants have acted intentionally and willfully within the meaning of 5 U.S.C. § 552a(g)(4). Defendants have repeatedly been alerted that the SCRA Website, as currently operated, violates the Privacy Act and puts veterans at risk of fraud, scams, and other injuries. They have failed to take any corrective action.

183. Plaintiff Barden has suffered adverse effects and direct out-of-pocket damages because of Defendants' refusal and failure to comply with these requirements.

184. In particular, Mr. Barden was victimized by con artists who perpetrated an impostor scam using information about his military service that Defendants make freely accessible through the SCRA Website.

185. As a result of the scam, Mr. Barden was defrauded of $300, which he paid to the scammer to purchase phony computer firewall software. Mr. Barden suffered additional out-of-pocket costs after the scammer took control of his computer and rendered it unusable. Mr. Barden spent $350 to purchase a replacement computer. These out-of-pocket costs constitute actual damages within the meaning of 5 U.S.C. § 552a(g)(4)(A).

186. Defendants' failure to implement appropriate technical and administrative safeguards (such as account registration and verification) and its failure to keep a proper accounting of disclosures through the SCRA Website make it difficult or impossible for Mr. Barden to identify the perpetrators of the scam or any others who have improperly accessed his Personal Information.

187. Plaintiff Barden is entitled to recover from Defendants the actual damages he suffered, and in no case less than $1000 per violation. 5 U.S.C. § 552a(g)(1)(D), (g)(4).

FOURTH CLAIM FOR RELIEF
Freedom of Information Act
(Failure to disclose records requested by Plaintiff Barden)

188. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

189. On June 9, 2017, Plaintiff Barden filed a Freedom of Information Act request with the DoD and its component DMDC seeking records regarding Defendants' disclosure of his Private Information through the SCRA Website.

190. The request seeks the following records:

a. A complete accounting of any and all disclosures of records pertaining to Mr. Barden that have been disclosed through the [SCRA Website].

b. All other records describing, listing, detailing, or otherwise documenting requests for Mr. Barden's information through the [SCRA Website] and any subsequent disclosures thereof, including but not limited to records that identify the IP addresses, company name, and username of individuals requesting and/or obtaining Mr. Barden's information as well as the date/time of each such request/disclosure.

191. The request was submitted to OSD/JS, which is responsible for processing requests for records in possession of DMDC. The request was also sent directly to DMDC's Privacy Act Branch. Both OSD/JS and DMDC are components of Defendant DoD.

192. DMDC acknowledged receipt of the request by letter dated June 16, 2017 and requested additional identifying information about Mr. Barden. By letter, dated June 23, 2017, DMDC acknowledged that it had received the perfected request on June 21, 2017. The letter further explained that DMDC would require an unspecified amount of additional time to process the request. The letter did not invoke any provision of FOIA that might permit an extension of the ordinary 20-business-day deadline for a response required by 5 U.S.C. § 552(a)(6)(A)(i).

193. By letter dated June 27, 2017, OSD/JS acknowledged that it received the request on June 20, 2017. The letter stated that DMDC's Privacy Act Branch would be responsible for processing the request; that DMDC had already received the request and begun processing; and that, as a result, OSD/JS was formally closing the request in its office.

194. More than twenty business days have elapsed since OSD/JS and DMDC received the request. Defendants have not produced any records responsive to the request or explained why any such records are properly withheld. Plaintiff Barden has thus constructively exhausted his administrative remedies. 5 U.S.C. § 552(a)(6)(C)(i).

195. Defendant DoD has failed to provide a timely response to Plaintiff Barden's request for records in violation of the Freedom of Information Act, 5 U.S.C. § 552(a)(6)(A), and DoD's corresponding regulations.

196. Defendant DoD has failed to make a reasonable effort to search for records responsive to Plaintiff Barden's request, in violation of FOIA, 5 U.S.C. § 552(a)(3)(C), and DoD's corresponding regulations.

197. Defendant DoD has failed to make available the records sought by Plaintiff Barden in violation of FOIA, 5 U.S.C. § 552(a)(3)(A), and DoD's corresponding regulations.

198. Defendant DoD's withholding of specific responsive records, or portions thereof, violates FOIA, 5 U.S.C. § 552(a)(3)(A), (6)(A), and DoD's corresponding regulations.

FIFTH CLAIM FOR RELIEF
Violation of Administrative Procedure Act
(Failure to eliminate use of SSNs on the SCRA Website, as required by the Federal Information Security Modernization Act and corresponding DoD policy)

199. Plaintiffs incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

200. Defendants' rules and procedures governing the SCRA Website permit users to run searches using an SSN in order to obtain an individual's Private Information. Defendants encourage users of the SCRA Website to use the SSN so as to improve the quality of search results.

201. These rules and procedures have an adverse effect on members of VVA, VVA NYSC, Chapter 77, including Plaintiff Barden, because they encourage third-party companies to require them to turn over their SSNs. Such disclosure of the SSN to third parties increases the

risk that their SSNs will be mishandled and misused, and puts them at risk of identity theft and other frauds.

202. Defendants' rules and procedures regarding the use of the SSN on the SCRA Website are inconsistent with DoD policy, particularly DoD Instruction 1000.30, as well as Office of Management and Budget ("OMB") policy, particularly OMB Circular A-130.

203. OMB Circular A-130 § 5(f)(1)(f) provides that "agencies shall take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier."

204. DoD Instruction 1000.30 strictly limits the circumstances in which DoD may use the SSN. It provides that "[a]ny uses of the SSN not provided for in this Instruction are considered to be unnecessary and shall be eliminated." The Instruction enumerates 13 categories of permissible uses of the SSN. None of these enumerated categories permits use of the SSN for the purpose of submitting requests on the SCRA Website, particularly as the Website is currently configured to be open to the public.

205. Defendants are under a statutory obligation to implement DoD Instruction 1000.30, as well as OMB Circular A-130. The Federal Information Security Modernization Act of 2014 ("FISMA") charges the Secretary of Defense with a non-discretionary duty for "complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including . . . policies and procedures issued by the Director [of the OMB]." 44 U.S.C. § 3554(a)(1)(B)(i).

206. With respect to DoD information systems, FISMA delegates the authority to issue binding policies from the Director of the OMB to the Secretary of Defense. 44 U.S.C. § 3553(e).

207. DoD Instruction 1000.30 is an information security policy within the meaning of FISMA, 44 U.S.C. §§ 3552(a)(3), 3553(a)(1), 3553(e)(1), 3554(a)(1)(B)(i). Defendants are subject to a non-discretionary duty to implement that policy pursuant to § 3554(a)(1)(B)(i). Defendants are also subject to a non-discretionary duty to implement OMB Circular A-130.

208. Defendants' rules and procedures permitting use of the SSN on the SCRA Website constitute final agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise contrary to law" under the APA, 5 U.S.C. § 706(a)(2), because they violate Defendants' obligation under FISMA to implement policies that forbid the use of SSN in these circumstances. Alternatively, Defendants' failure to eliminate use of the SSN for purposes of the SCRA Website constitutes agency action "unlawfully withheld" within the meaning of the APA, 5 U.S.C. § 706(1).

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

(1) Declare that the SCRA Website, as currently operated, violates the APA and the Privacy Act by permitting unlawful disclosure of private information; by failing to implement adequate safeguards to protect private information; and by failing to keep a proper accounting of disclosures of private information.

(2) Enjoin Defendants from disclosing information in response to queries of the SCRA Website as currently operated.

(3) Direct, by issuance of an injunction, that Defendants keep an accounting of each and every disclosure through the SCRA Website that includes, at a minimum, the name and address of those to whom information is disclosed and the nature and purpose of each disclosure.

(4) Direct, by issuance of an injunction, that Defendants implement access controls and other safeguards that ensure, at a minimum, that Private Information can only be obtained through the SCRA Website by users who are regulated by the SCRA and who seek disclosure for the sole purpose of determining whether an individual is entitled to SCRA protection.

(5) Declare that Defendants have violated the APA and Privacy Act by unlawfully disclosing private information about Mr. Barden and others whose details are accessible through the SCRA Website.

(6) Award to Mr. Barden damages in an amount to be determined by the Court not less than $1000.

(7) Order the Department of Defense immediately to disclose to Mr. Barden all of the records he has requested, without redaction.

(8) Declare that it is unlawful for Defendants to permit use of the SSN to query the SCRA Website.

(9) Enjoin Defendants' from permitting or encouraging use of the SSN to query the SCRA Website

(10) Award Plaintiffs' costs and reasonable attorneys' fees incurred in this action pursuant to the Equal Access to Justice Act, 28 U.S.C. § 2412, the Privacy Act, 5 U.S.C. § 552a(g)(4)(B); and the Freedom of Information Act, 5 U.S.C. § 552(a)(4)(E)(i).

(11) Grant any other relief as this Court may deem just and proper.

Dated: August 1, 2017
Buffalo, New York

Respectfully submitted,

s/Jonathan Manes

Jonathan Manes, *Supervising Attorney*
Jessica Gill, *Student Attorney*
Arthur Heberle, *Student Attorney*
Thora Knight, *Student Attorney*
Attorneys for the Plaintiffs[*]
Civil Liberties and Transparency Clinic
University at Buffalo School of Law
507 O'Brian Hall, North Campus
Buffalo, New York 14260-1100
Tel: (716) 645-2167
Fax: (716) 645-6199
jmmanes@buffalo.edu

[*] An application pursuant to this Court's student practice rule is forthcoming with respect to the student attorneys listed here. Plaintiffs wish to recognize and thank Laura Gardiner, Kristian Klepes, Megan Knepka, and Larry Waters for their assistance.