UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION This Document Relates To: ALL CASES	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664

FIRST AMENDED CONSOLIDATED COMPLAINT

I. NATURE OF THE ACTION

1. This action arises from the failure of Defendants the United States Office of Personnel Management ("OPM") and its security contractor Peraton Risk Decision Inc. ("Peraton"), to establish legally required safeguards to ensure the security of government investigation information of current, former, and prospective employees of the federal government and its contractors. Defendants' failure to implement adequate, compulsory security measures in the face of known, ongoing, and persistent cyber threats—and despite repeated warnings of their systems' vulnerabilities—resulted in data breaches affecting more than 21 million people. The government investigation information ("GII") exposed and stolen in these breaches is private and sensitive, consisting of fingerprint records, detailed personal, financial, medical, and associational histories, Social Security numbers and birthdates of employees and their family members, and other private facts collected in federal background and security clearance investigations and stored on Defendants' electronic systems.

2. OPM announced a series of data breaches in 2015. For years before the announcement, OPM officials knew that OPM's systems lacked critical security safeguards and controls. Since 2007, audits carried out by the Office of Inspector General ("IG"), an independent office within OPM, warned that OPM's information security systems, management, and protocols were inordinately lax and vulnerable to electronic incursions. The OPM Inspector General's audits determined that OPM lacked not only the technology and oversight to protect its systems from cyberattacks but also the ability to discern the existence and extent of such an attack. OPM failed to remedy these known deficiencies and failed to follow its auditors' guidance for bringing its cybersecurity defenses into compliance with federal requirements.

3. OPM officials knew that OPM was a prime target for cyberattacks. OPM officials were aware of constant hacking attempts against OPM's systems. OPM's systems were breached in 2009 and 2012. A November 2013 attack compromised critical security documents.

4. Then in about December 2013, an unknown person or persons obtained the user log-in credentials of a Peraton employee. Those credentials were used to invade Peraton's systems and steal the personnel records of tens of thousands of Department of Homeland Security employees (the "Peraton Breach").

5. OPM learned in September 2014 of the December 2013 cyberattack on Peraton. OPM did not terminate or suspend its contract with Peraton, limit Peraton's access to OPM's systems, or take remedial actions necessary to protect OPM's systems from incursions made possible by the Peraton Breach.

6. Hackers used Peraton credentials to breach OPM's information systems in May 2014 and maintained access to OPM's information systems for over a year. Once inside OPM's network, the hackers gained access to another set of OPM servers stored in the Interior

Department. The attacks begun in 2014 (the "OPM Breaches") went undetected for several months. By the time they were discovered, vast amounts of sensitive information had been extracted from OPM's network.

7. The victims of the Peraton Breach and the OPM Breaches (together, the "Data Breaches") have sustained economic harm from misuse of the stolen information, and their GII remains subject to a continuing risk of additional exposure or theft as a consequence of OPM's failure to secure it.

8. Defendants' failure to protect GII, despite repeated official warnings of cyber threats and security lapses in their systems, constitutes willful misconduct. OPM, unlawfully prioritizing convenience over safety and ignoring direction from its federal auditors, violated the Privacy Act, the Federal Information Security Management Act, and the Federal Information Security Modernization Act. Peraton's actions and inactions constitute negligence and violate state consumer protection statutes.

II. PARTIES

A. Plaintiffs

9. As used in this Complaint, "sensitive personal information" includes, at a minimum, Social Security numbers and birthdates, but may also include the range of GII compromised in the Data Breaches.

10. Plaintiff Travis Arnold resides and is domiciled in the state of Arizona. He formerly served in Field Artillery at the Department of Defense for approximately twelve years. Arnold provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Upon being informed of the Data Breaches, Arnold purchased credit monitoring

services from LifeLock, for which he paid $10 per month. He later switched to Experian credit monitoring and continues to pay approximately $10 per month for that service. In May 2015, while reviewing his bank statement, Arnold discovered an unauthorized charge of approximately $125 for a purchase in China. He has spent approximately ten hours communicating with employees of his bank to reverse this fraudulent transaction and submitting documents detailing the fraud. While reviewing his credit report, Arnold also learned that between six and ten inquiries regarding his credit had been made by companies with which he had no prior relationship. Arnold has spent many hours disputing these fraudulent inquiries. He suffers stress related to concerns for his personal safety and that of his family members. His exposure to the Data Breaches has also caused Arnold to review his credit reports and financial accounts with greater frequency.

11. Plaintiff Tony Bachtell resides and is domiciled in the state of Wisconsin. He currently works as a floor covering specialist at Orion Hardwood Floors, a federal government contractor. Bachtell provided sensitive personal information to the federal government. He and his wife received notice from OPM that such information has been compromised in the Data Breaches. After receiving this notification, Bachtell paid to freeze his credit and signed up for the credit monitoring service offered by OPM. In February 2016, the IRS informed Bachtell that a fraudulent tax return for the 2015 tax year had been filed using his and his wife's personal information. Bachtell spent many hours attempting to resolve this tax fraud issue. Payment of his tax refunds were delayed for several months. Also in February 2016, the Social Security Administration informed Bachtell that an unknown individual had used his and his wife's personal information to create online "My Social Security" accounts. Such accounts can be used to request a replacement Social Security card and to obtain estimates of a Social Security

cardholder's future retirement benefits and the amount he or she has paid in Social Security and Medicare taxes. Thereafter, Bachtell learned that approximately ten inquiries regarding his credit had been made by companies with which he had no prior relationship. Bachtell has devoted many hours to remedial actions, including communicating with the Social Security Administration to terminate the unauthorized accounts. His exposure to the Data Breaches has also caused Bachtell to review his credit reports and financial accounts with greater frequency.

12. Plaintiff Gardell Branch resides and is domiciled in the state of Illinois. He formerly worked as a Casual Mail Handler at the Postal Service. Branch provided sensitive personal information to the federal government, including in an SF-85 form, and received notice from OPM that such information has been compromised in the Data Breaches. Branch thereafter purchased monthly credit monitoring services from Equifax at a rate of $8.95 per month. Additionally, the Social Security Administration notified Branch that an unknown individual had attempted to use his Social Security Number. This incident required Branch to spend time verifying his identity and creating an identity theft profile with the Social Security Administration. In 2015, Bank of America informed Branch that an unknown individual had tried to open an account in his name, an incident that required Branch to spend time replacing his debit and credit cards. Branch took time off work to visit a Bank of America branch and spent money on gas to drive to the branch. His exposure to the Data Breaches has also caused Branch to review his financial accounts with greater frequency. He now reviews his bank and credit card accounts at least every other day to detect fraudulent activity.

13. Plaintiff Myrna Brown resides and is domiciled in the state of New Mexico. She formerly worked as an International Trade Specialist in the Foreign Commercial Service of the Commerce Department. Brown provided sensitive personal information to the federal

government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. In 2015, Brown discovered fraudulent activity on her credit card account. She later purchased a credit monitoring service. Her exposure to the Data Breaches has caused Brown to review her financial accounts with greater frequency. Brown now also reviews her credit reports regularly to detect fraudulent activity. Additionally, Brown suffers stress resulting from fear that the theft of her sensitive personal information will impair her ability to obtain future federal government employment or security clearances, and fear for the safety of her family members who serve in the military.

14. Plaintiff Lillian Colon-McKnight resides and is domiciled in the state of Florida. She currently works as an Industrial Hygienist at the Department of Labor. She previously worked as a Medical Technologist at the Department of Veterans Affairs. Colon-McKnight provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In December 2014, Colon-McKnight learned that a series of inquiries regarding her credit had been made in connection with an unauthorized attempt to open fraudulent accounts in her name. In January 2015, the IRS informed Colon-McKnight that an unknown individual had fraudulently claimed her 4-year-old son as a dependent on a tax return filed in New York for the 2014 tax year. As a result, payment of her tax refunds was delayed for three months. In February 2016, Colon-McKnight's mortgage lenders informed her that an account with Verizon Wireless had been opened in her name in December 2014 and that this account had an outstanding balance of almost $3,000. To address the fraud, Colon-McKnight had to mail Verizon her tax returns and proof of residence, which cost her postage fees. Colon-McKnight spent over 100 hours in attempts to resolve the fraudulent tax return filing and to close the fraudulent Verizon Wireless

account. These efforts required her to take time off work and spend money on gas driving to the IRS offices in Tampa, Florida and to Social Security Administration offices to submit paperwork and verify her identity. Her exposure to the Data Breaches has caused Colon-McKnight to review her credit reports and financial accounts with greater frequency. Colon-McKnight suffers stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future.

15. Plaintiff Paul Daly resides and is domiciled in the state of Florida. He formerly worked as a Manager of Distribution Operations at the Postal Service, where he was employed for approximately 37 years. Daly's wife formerly worked at the IRS. Daly and his wife provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In April 2015, the IRS informed Daly that fraudulent tax returns for the 2014 tax year had been filed using his and his wife's personal information (on separate tax return forms). Daly has spent many hours attempting to resolve these tax fraud issues. Following the recommendations of the IRS, Mr. Daly filed a complaint with the FTC and a police report with the local sheriff. Additionally, he closed financial accounts and opened new ones, and purchased credit monitoring services through Equifax, for which he pays $29.95 per month. He later switched to credit monitoring services offered by Discover and continues to pay for those services. His exposure to the Data Breaches has also caused Daly to review his financial accounts with greater frequency, and to refrain from online bill payment activities, which has caused him to incur $30.95 per month in fees to make payments over the phone for his wife's car and for their credit card and phone bills.

16. Plaintiff Jon Decker resides and is domiciled in the state of Virginia. Decker is an independent contractor who works with a federal government contractor. He previously served

in the Army. Decker provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. The IRS thereafter informed Decker that a fraudulent tax return had been filed using his personal information. Decker spent several hours attempting to resolve this tax fraud issue. Payment of his tax refunds was delayed and the IRS required him to submit his taxes by mail, which caused him to incur postage expenses. In 2016, Decker learned that someone had applied for a U.S. Bank credit card in his name. He had to spend time addressing this fraud, including by working with Equifax to remove the credit inquiry from his credit report. His exposure to the Data Breaches has also caused Decker to review his financial accounts with greater frequency. He now spends approximately one hour per day reviewing his financial accounts in order to detect fraudulent activity.

17. Plaintiff Jane Doe currently resides in Tennessee. She is using the pseudonym "Jane Doe" in this action because of her personal safety concerns. Doe currently works as an Information Technology Specialist Project Manager at the Department of Defense. She formerly worked at various federal agencies in positions that similarly involved monitoring and controlling computer systems. Doe's husband serves in the Army. Doe and her husband each provided sensitive personal information to the federal government, including in SF-86 forms. Doe and her husband each received notice from OPM that such information has been compromised in the Data Breaches. In August 2015, the Federal Bureau of Investigation informed Doe that her GII had been acquired by the so-called Islamic State of Iraq and al-Sham ("ISIS"). In response, Doe purchased a comprehensive home security system for $5,000 to protect her family and pays a $39 monthly fee for operation of the security system. While reviewing her credit report, Doe discovered that twelve unknown accounts had been fraudulently

opened in her name and were in collections. She paid approximately $198 to a credit repair law firm for assistance in closing the fraudulent accounts and removing them from her credit report. When Doe attempted to access her credit report online with TransUnion, she found that she was unable to do so because TransUnion could not verify her identity. Doe has spent between 40 and 50 hours dealing with the fraudulent accounts, communicating with the FBI, and attempting to gain access to her credit report with TransUnion. She spent approximately $50 to obtain copies of her credit report and also paid $15 to place a security freeze with each credit bureau. Doe suffers stress resulting from concerns for her personal safety and that of her family members, and concerns that her exposure to the Data Breaches will impair her ability to obtain a job transfer and the Top Secret clearance needed to perform her job. Her exposure to the Data Breaches has also caused Doe to review her credit reports and financial accounts with greater frequency.

18. Plaintiff Jane Doe II resides and is domiciled in the state of Kansas. She is using the pseudonym "Jane Doe II" in this action because of her personal safety concerns. Doe II's spouse is an Assistant United States Attorney responsible for prosecuting large-scale narcotics and money laundering cases, including cases against international drug cartels known to target prosecutors, law enforcement officials, and their families. Doe II's husband has received multiple death threats throughout his career and was the subject of an assassination attempt. Since that attempt, Doe II and her husband have used a P.O. Box miles from their home as their mailing address, and have maintained unlisted telephone numbers. Doe II and her husband have two minor children. Doe II's husband provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Doe II also received notice from OPM that her sensitive personal information has been compromised in the Data Breaches. Doe II and her

husband paid over $1,500 to upgrade their home security system in response to the Data Breaches. Doe II experiences significant stress from fear that the exposure of her and her family members' sensitive personal information will cause them to be targeted for retaliatory attacks and bodily harm. Doe II also experiences stress from concerns that she and her family members face an increased risk of identity theft, fraud, and other types of monetary harm.

19. Plaintiff John Doe II resides and is domiciled in the state of Oklahoma. He is using the pseudonym "John Doe II" in this action because of his personal safety concerns. He formerly worked for 20 years as a Senior Special Agent with the Customs Service, Office of Enforcement (which merged with Immigration and Naturalization Service, Investigations to form Immigration and Customs Enforcement, a division of the Department of Homeland Security, and was later renamed Homeland Security Investigations). As a member of the Joint Terrorist Task Force, Doe II supervised investigations of terrorism and drug trafficking cartels. His security clearance was above Top Secret, at the Sensitive Compartmented Information level. Doe II provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. He thereafter spent time to change his bank accounts, and he purchased credit monitoring services through LifeLock, for which he has paid a total of $708.45. Doe II suffers stress resulting from concerns for his personal safety and that of his family members. His exposure to the Data Breaches has also caused Doe II to review his credit reports and financial accounts with greater frequency.

20. Plaintiff Kelly Flynn resides and is domiciled in the state of Utah. She currently works as a Staff Assistant at the Interior Department's Office of the Solicitor. She formerly worked at the Air Force, the Navy, the IRS, and the Postal Service. Flynn provided sensitive

personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In July 2015, after learning of the Data Breaches, Flynn added credit monitoring from the three major credit bureaus, at a cost of $10 per month, to her preexisting credit and identity monitoring services. Flynn thereafter learned that a Barclays Bank credit card and a JCPenney credit card had been fraudulently opened in her name. Flynn's husband also learned that two credit card accounts had been fraudulently opened in his name. Additionally, Equifax notified Flynn that a $5,000 loan from Cash Central had been taken out in her name online, and that the loan was delinquent and in collections. Flynn had to call the police and file a police report because Cash Central required such a report before it would accept that the loan was fraudulent. On March 1, 2016, Flynn's husband learned that a loan of over $1,400 with Castle Creek Payday Loans had been taken out in his name online, and was delinquent. Flynn then signed up for LifeLock credit monitoring services, for which she paid $29.99 per month until March 2019. In spring 2015, the IRS informed Flynn that a fraudulent tax return for the 2014 tax year had been filed using her and her husband's personal information. As a result, Flynn's tax refund was delayed. Fraudulent tax returns again were filed in Flynn's name in 2016 and 2017. As a result, she was required to submit her tax returns on paper and by mail, which cost her postage fees. Flynn has spent over 50 hours attempting to resolve the tax fraud issues and to close the fraudulent accounts and terminate the fraudulent loans. Her exposure to the Data Breaches has also caused Flynn to review her credit reports and financial accounts with greater frequency. Flynn suffers stress resulting from concerns that her and her family members' identities will be stolen.

21. Plaintiff Alia Fuli resides and is domiciled in the state of Nevada. She currently works as a Service Representative at the Social Security Administration, and formerly worked as

a Medical Reimbursement Technician and Patient Accounts Representative at the Department of Veterans Affairs. Fuli began working for the Department of Veterans Affairs in 2011. Fuli provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In December 2015, Fuli learned that a PayPal/Synchrony Bank credit card account had been opened in her name and used to make unauthorized online purchases of approximately $298. In an attempt to get these charges reversed and the fraudulent account closed, Fuli spent approximately 15 hours communicating with PayPal representatives and also paid for postage to send proof of her identity. While reviewing her credit report, Fuli also learned that between July 2015 and December 2015, multiple inquiries regarding her credit had been made by companies with which she had no prior relationship. These inquiries caused her credit score to drop significantly. Her exposure to the Data Breaches has caused Fuli to review her credit reports and financial accounts with greater frequency.

22. Plaintiff Johnny Gonzalez resides and is domiciled in the state of Florida. He currently works as a Deportation Officer at Immigrations and Customs Enforcement, and formerly worked as a Border Patrol Agent at Customs and Border Protection. Gonzalez provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Gonzalez's bank thereafter informed him that his debit card number had been used to make unauthorized charges of approximately $360 in China. In January 2016, Gonzalez's bank informed him that an unauthorized attempt had been made to charge approximately $1,000 on his debit card, and that an additional $96 in unauthorized charges had been approved and deducted from his checking account. In late 2015, Gonzalez also learned that his credit card had

been used to make an unauthorized charge of approximately $100. Gonzalez spent approximately 50 hours addressing the fraudulent activity and had to take time off work. Gonzalez suffers stress resulting from concerns that his exposure to the Data Breaches will impair his ability to renew his current security clearance and/or to obtain a higher security clearance in the future. His exposure to the Data Breaches has also caused Gonzalez to review his financial accounts with greater frequency.

23. Plaintiff Orin Griffith resides and is domiciled in the state of Oklahoma. Griffith currently serves as an Aircraft Mechanic in the Air Force, and formerly served as an Aircraft Weapons Mechanic in the Army. Griffith provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. After learning of the Data Breaches, Griffith placed a security freeze on his personal credit and signed up for the credit monitoring service offered by OPM. In February 2015, the IRS informed Griffith that a fraudulent tax return for the 2014 tax year had been filed using his and his wife's personal information. Griffith has spent about 30 hours attempting to resolve this tax fraud issue and had to take time off work. He must now submit his tax returns on paper and by mail, which requires that he pay for postage. Payment of his tax refunds was delayed for almost ten months. Griffith's exposure to the Data Breaches has caused him to review his financial accounts with greater frequency.

24. Plaintiff Jennifer Gum resides and is domiciled in the state of Kansas. She works as a Medical Reimbursement Technician for the Veterans Affairs Medical Center, and her husband works as a Senior Corrections Officer with the Federal Bureau of Prisons. She began working for the Department of Veterans Affairs in 2011. Gum and her husband provided sensitive personal information to the federal government and received notice from OPM that

such information has been compromised in the Data Breaches. Upon learning of the Data Breaches, Gum spent several hours signing up for the credit monitoring service offered by OPM and changing passwords to her accounts. Additionally, shortly after the Data Breaches, Gum discovered that an unknown and unauthorized individual had accessed her bank account to make fraudulent purchases. She incurred costs and spent several hours working with her bank to reverse the charges. Her exposure to the Data Breaches has caused Gum to worry that her children's information will be compromised and also to review her accounts with greater frequency.

25. Plaintiff Michael Hanagan resides and is domiciled in the state of California. He previously worked as a Capital Habeas Staff Attorney in the United States District Court for the Central District of California. Hanagan provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Hanagan thereafter purchased a monthly subscription for credit and identity monitoring and purchased copies of his credit reports to detect fraudulent activity. Hanagan paid $40 per month for 12 months for credit monitoring services from Experian. Additionally, after the Data Breaches, Hanagan discovered fraudulent charges on his debit card and spent several hours working with his bank to have them reversed.

26. Plaintiff Deborah Hoffman resides and is domiciled in New Mexico. She currently works as a transcriptionist with Datagain, a federal government contractor. Hoffman provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Upon learning of the Data Breaches, Hoffman purchased credit monitoring services. Her exposure to the Data Breaches has also caused Hoffman to review her financial accounts

with greater frequency. She now checks her bank and credit card accounts daily to detect fraudulent activity.

27. Plaintiff Cynthia King-Myers resides and is domiciled in the state of Illinois. She is currently employed as a Social Worker at the Department of Veterans Affairs. She began working for the Department of Veterans Affairs in 2013. King-Myers provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In May 2015, King-Myers learned that unauthorized charges of approximately $658 had been incurred on her bank account. Around the same time, unauthorized charges totaling about $260 were incurred on King-Myers's daughter's bank account, which is linked to hers. Then in November 2015, her daughter's account experienced further unauthorized charges of $100. King-Myers has spent between 30 and 35 hours attempting to reverse these fraudulent transactions. She also purchased a subscription to Experian's monthly credit monitoring service, for which she pays a monthly fee. Her exposure to the Data Breaches has also caused King-Myers to review her credit reports and financial accounts with greater frequency.

28. Plaintiff Todd Kupferer resides and is domiciled in the state of Washington. He worked as a Deputy U.S. Marshall, Senior Inspector with the Marshals Service, where he was employed for approximately 27 years. Kupferer holds a Top Secret clearance and has investigated drug trafficking cartels. Kupferer provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In February 2016, the IRS informed Kupferer that a fraudulent tax return for the 2015 tax year had been filed using his and his wife's personal information. Kupferer spent approximately 50 hours and $50 attempting to resolve this tax fraud issue, including

payments for gas to drive to an IRS office. Payment of his tax refunds was delayed for several months, and Kupferer had to file his tax returns on paper, requiring payments for postage. Kupferer suffers stress resulting from concerns for his personal safety and that of his family members, and concerns that identity theft will aggravate his health problems and adversely affect his retirement plan.

29. Plaintiff Ryan Lozar resides and is domiciled in the state of New York. He formerly worked as a Law Clerk in the United States District Court for the Eastern District of New York, a Law Clerk in the United States District Court for the District of Puerto Rico, and a Special Assistant United States Attorney in the United States Attorney's Office for the Southern District of California. Lozar provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Lozar thereafter learned that an unknown individual had opened a PayPal account in his name and received a $1,000 cash advance. He also learned that an unknown individual had opened a Best Buy account in his name and used it to purchase $3,500 worth of merchandise. Lozar spent many hours communicating with PayPal and Best Buy to dispute and resolve these fraudulent activities. Lozar then paid $15 to place a freeze on his credit and contacted the three major credit bureaus to confirm that they were aware of the fraud. Lozar still has a freeze on his credit, and each time he wants to use a line of credit, he must temporarily lift the freeze. This process requires him to call his credit card company, pay $5, and then get a special PIN for third parties to access his credit card information.

30. Plaintiff Teresa J. McGarry resides and is domiciled in the state of Florida. She currently works in the Social Security Administration as an Administrative Law Judge. McGarry previously served as an Assistant United States Attorney and as a Judge Advocate General with

the Navy. McGarry provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. McGarry thereafter purchased a monthly subscription for credit and identity monitoring, which costs her $7.95 per month. In 2019, McGarry's information was used by an unknown individual to apply for a mortgage loan, which prompted McGarry to file a report with the FBI. She spent hours on the phone with various banks, financial companies, and the FBI. Her exposure to the Data Breaches has also caused McGarry to review her financial accounts with greater frequency.

31. Plaintiff Charlene Oliver resides and is domiciled in the state of Mississippi. She works as a Claims Assistant at the Veterans Benefits Administration and formerly worked for the Postal Service as well as serving in the Navy, as a Torpedoman's Mate. Oliver's husband formerly served in the Army, as a Captain of Artillery. Oliver and her husband provided their sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Thereafter, Oliver purchased credit monitoring, which cost her $40 per month. In June 2015, Oliver received a letter from her electricity utility company informing her that her account had been closed, was no longer in her name, and had incurred charges of $500. Oliver also learned that an unknown individual had accessed her electricity account online using her Social Security number and maiden name. Oliver has devoted many hours to communicating with her electricity utility company to reverse the fraudulent charges and reopen an account in her name. Among other expenditures, Oliver had to pay a $396 deposit to restore her electricity. Her exposure to the Data Breaches has also caused Oliver to review her financial accounts with greater frequency.

32. Plaintiff Mario Sampedro resides and is domiciled in the state of California. For 27 years, he worked as a Special Agent at the Department of Homeland Security and with the Customs Service. Sampedro provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. In 2015 and again in 2016 Sampedro suffered incidents of identity fraud. Additionally, during the evening of October 15 and the morning of October 16, 2016, Google notified Sampedro that there had been suspicious activity on and an unauthorized person was trying to access his Google accounts. Over the course of the identity theft incidents, Sampedro spent approximately three days working with his banks and Google to remediate the fraudulent activity, and he incurred gas costs when traveling to bank branches as well as other related costs, including for postage. Sampedro suffers stress resulting from concerns for his personal safety and that of his family members, and concerns regarding the unauthorized use of their sensitive personal information. Sampedro, who is nearing retirement from Homeland Security, worries that the theft of his sensitive personal information will impair his ability to secure future employment with government contractors. His exposure to the Data Breaches has caused Sampedro to review his financial accounts with greater frequency.

33. Plaintiff Zachary Sharper resides and is domiciled in the state of Virginia. He currently works as a Contract Specialist Supervisor with the Department of Defense, Defense Logistics Agency. Sharper previously worked as a Corrections Officer at the Bureau of Prisons and a Fuel Systems Operator for the federal government contractor Kellogg Brown & Root. Additionally, Sharper served in the Army for approximately seven years. He provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Sharper

thereafter learned accounts had been opened in his name with Sprint and Verizon Wireless, and that six iPhones had been ordered using those accounts. Sharper also received prepaid Green Dot cards he had not ordered. He has spent many hours attempting to resolve these fraudulent transactions, and incurred postage costs to send documentation confirming his identity.

34. Plaintiff Robert Slater resides and is domiciled in the state of Washington. He currently works for Lockheed Martin and previously served as a Signal Officer, and as a Patriot Missile Operator, in the Army. Slater provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Slater discovered unauthorized debit card transactions in 2016 and spent time working with his bank to reverse the charges. He later purchased credit monitoring to prevent and identify future identity fraud. His exposure to the Data Breaches has also caused Slater to review his financial accounts and credit reports with greater frequency to detect fraudulent activity.

35. Plaintiff Nancy Wheatley resides and is domiciled in the state of Tennessee. She currently works as a registered nurse at the Department of Veterans Affairs. She began working for the Department of Veterans Affairs in 2011, and formerly served in the Army and in the National Guard. Wheatley provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. She thereafter learned that unknown individuals had opened fraudulent accounts in her name with Sprint and Virgin Mobile and that unauthorized online purchases had been made using her debit card number. To prove that the accounts were opened fraudulently, she had to file a police report, which required a fee, and she also paid for postage and certified mailing costs. Wheatley spent over 24 hours working to close the fraudulent

accounts and to reverse the fraudulent transactions. Her exposure to the Data Breaches has also caused Wheatley to review her financial accounts with greater frequency.

36. Plaintiff Kimberly Winsor resides and is domiciled in the state of Kansas. She is currently employed as a Social Worker at the Department of Veterans Affairs in Kansas City. She began working for the Department of Veterans Affairs in 2015. Winsor and her husband provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In April 2015, Winsor's husband learned from their bank that his debit card number had been used to make unauthorized purchases in Mississippi. On July 23, 2015, Winsor learned from their bank that her debit card number had been used to make unauthorized purchases in Texas. On November 24, 2015, CSID informed Winsor that her 8-year-old son's Social Security number had been used in California for an unknown purpose. Winsor has spent approximately 35 hours to resolve the fraudulent transactions and the misuse of her son's Social Security number, which required her to take time off work and incur postage costs in mailing proof of her and her son's identity. She also made trips to her bank to obtain sensitive identifying documents, and completed and submitted affidavits to dispute the fraudulent purchases. Winsor suffers stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future. Her exposure to the Data Breaches has also caused Winsor to review her financial accounts with greater frequency.

B. Defendants

37. Defendant U.S. Office of Personnel Management is a federal agency headquartered at 1900 E Street, N.W., Washington, D.C. 20415. OPM handles many parts of the federal employee recruitment process and, in doing so, collects and maintains federal job

applicants' GII, including information provided in background check and security clearance forms. OPM oversees more than two million background checks annually, provides human resources services to other agencies, and audits agency personnel practices.

38. Defendant Peraton—previously KeyPoint Government Solutions, Inc. and Perspecta Risk Decision Inc.—is a private investigation and security firm incorporated in Delaware. Peraton is headquartered and maintains its principal place of business in Loveland, Colorado. Peraton provides fieldwork services for federal background and security clearance checks and employs or contracts with individuals in every state who assist with such investigations.

III. JURISDICTION AND VENUE

39. The Court has subject matter jurisdiction over the Privacy Act claim pursuant to 5 U.S.C. § 552a(g)(1)(D) and 28 U.S.C. § 1331.

40. This Court has subject matter jurisdiction over the claims against Peraton pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because Plaintiffs bring class claims on behalf of citizens of states different from Peraton's state of citizenship, the total amount in controversy exceeds $5 million, and the proposed Class contains more than 100 members.

41. This Court has personal jurisdiction over OPM because it is headquartered in the District of Columbia and much of the relevant conduct occurred here.

42. This Court has personal jurisdiction over Peraton because it conducts significant business in the District of Columbia and much of the relevant conduct occurred here.

43. Venue is proper in this District under 28 U.S.C. § 1391 because OPM is located in the District of Columbia and a substantial part of the events and omissions giving rise to these claims occurred here.

44. Venue is also proper in this District under 5 U.S.C. §§ 552a(g)(5) and 703.

IV. COMMON ALLEGATIONS OF FACT

A. OPM and Peraton Collect and Store Confidential Information About Millions of Federal Job Applicants

45. OPM manages the recruitment and retention of the work force of the United States government. As part of its duties, OPM conducts background checks of prospective employees and security clearance checks of current and prospective employees. More than 100 federal agencies depend on OPM's investigatory products and services. OPM oversees more than two million investigations per year, at least 650,000 of which are to support security clearance determinations.

46. As part of its investigatory mandate, OPM collects and stores an enormous amount of information about federal job applicants and past and present federal employees.

47. OPM's Federal Investigative Services division oversees the agency's background and security clearance checks.

48. Federal Investigative Services relies on a software system known as "EPIC." EPIC aggregates and stores information about federal job applicants, including information provided in electronic questionnaires and used in background and security clearance checks. Some of the data in EPIC is sufficiently sensitive that it is housed at the National Security Agency.

49. Among the data stored in EPIC are the master records from investigations of government employees.

50. EPIC also stores the Central Verification System, which contains most background and security clearance check information.

51. The Central Verification System stores versions of Standard Form 86 ("SF-86") as completed by federal job applicants and employees. SF-86 is a 127-page form that every federal job applicant and employee being considered for a security clearance must fill out and submit.

52. SF-86 contains, among other information, applicants' psychological and emotional health history, police records, illicit drug and alcohol use history, Social Security numbers, birthdates, financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, names of neighbors and close friends (such as college roommates and co-workers), and the Social Security numbers and birthdates of spouses, children, and other cohabitants.

53. Each SF-86 form states that the information provided in it "will be protected from unauthorized disclosure." Each SF-86 form also states that the information provided in it "may be disclosed without your consent . . . as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses." Form SF-86 lists eleven permitted uses.

54. Applicants for non-sensitive federal government or contractor positions must fill out and submit an SF-85 form. Each SF-85 form states that the information provided in it "will be protected from unauthorized disclosure." Each SF-85 form also states that the information provided in it "may be disclosed without your consent . . . as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses." Form SF-85 lists eleven permitted uses.

55. Applicants for "public trust" federal government or contractor positions must fill out and submit an SF-85P form. Each SF-85P form states that the information provided in it

"will be protected from unauthorized disclosure." Each SF-85P form also states that the information provided in it "may be disclosed without your consent . . . as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses." Form SF-85P lists eleven permitted uses.

56. The Central Verification System stores completed versions of forms SF-85 and SF-85P.

57. The Central Verification System also contains polygraph data, fitness determinations, and decisions made pursuant to Homeland Security Presidential Directive (the background check determinations required for government employees and contractors to gain access to federal facilities).

58. Additionally, the Central Verification System contains detailed information relating to Personal Identification Verification ("PIV") Cards, which are government ID smart cards that government employees and contractors use to access government facilities and software systems.

59. The Electronic Official Personnel Folder is another OPM system that stores personnel files on individual federal employees. The information in such files includes birth certificates, job performance reports, resumes, school transcripts, military service records, employment history and benefits, and job applications that contain Social Security numbers and birthdates.

60. OPM hires contractors to carry out the investigative fieldwork necessary for background and security clearance investigations. Peraton performs the majority of OPM's fieldwork. As a contractor of OPM, Peraton is subject to the requirements of the Privacy Act to the same extent as OPM. As of June 2015, Peraton had received more than $605 million under its OPM contract, with a funding cap of approximately $2.5 billion.

61. To perform its fieldwork, Peraton relies on systems that are electronically connected to those of OPM. This linkage allows Peraton employees and contractors to download from OPM's network information needed to conduct an investigation, and to upload investigatory findings to OPM's network. The system through which Peraton transmits data to and from OPM's network is called the Secure Portal. The Secure Portal is an electronic conduit through which, among other things, Peraton investigators access completed forms and other information stored in OPM's Central Verification System.

62. Peraton disseminates its Privacy Policy on the Internet. The policy states that Peraton is a consumer reporting agency. The policy further states that Peraton is required by the Fair Credit Reporting Act, 15 U.S.C. § 168, *et seq.* ("FCRA"), to maintain the confidentiality of all consumer information. Peraton's Privacy Policy states that Peraton safeguards confidential consumer information from unauthorized internal and external disclosure, by maintaining a secure network, limiting access to Peraton's computer terminals and files, and maintaining backup data in encrypted form.

B. OPM's Prior Data Breaches and Failures to Comply with Federal Cybersecurity Standards and Audit Directions

63. At least two cyberattacks against OPM were publicly disclosed in the years leading up to the Data Breaches. In 2009, OPM's website and database for USAJOBS.gov—the employment website used by the federal government—was hacked by unknown persons who gained access to millions of users' private information. In May 2012, an unknown person or group infiltrated an OPM database, stole OPM user credentials (including user IDs and passwords), and posted those credentials online.

64. In addition to these cyberattacks, OPM was and is aware that its network is the subject of at least 10 million unauthorized electronic intrusion attempts every month.

65. At all relevant times, OPM also was aware of several successful cyberattacks against other federal agencies and government institutions. OPM was aware of at least the following data breach incidents: a May 2012 hack into the Bureau of Justice Statistics of the Department of Justice, a May 2012 hack of the Thrift Savings Plan, a June 2012 hack of the Commodity Futures Trading Commission network, a June 2012 incursion into a Department of Homeland Security website, and a September 2012 breach of personnel data maintained by the Navy.

i. The Inspector General's Annual FISMA Audits of OPM

66. From 2002 to 2014, the Federal Information Security Management Act governed software system requirements for federal agencies and contractors. 44 U.S.C. § 3541, *et seq.* The President signed the Federal Information Security Modernization Act of 2014 into law on December 18, 2014. That statute updates and supersedes the Federal Information Security Management Act. As used in this Complaint, "FISMA" means either the Federal Information Security Management Act of 2002 or the Federal Information Security Modernization Act of 2014, or both.

67. FISMA requires OPM to develop and implement policies, procedures, and guidelines on information security, and to comply with federal information security standards that FISMA makes compulsory and binding on OPM.

68. Agencies subject to FISMA must develop, implement, and maintain a security program that assesses information security risks and provides adequate security for the operations and assets of programs and software systems under agency and contractor control.

69. The IG, an independent office within OPM, conducts annual audits of OPM's cybersecurity program and practices in accordance with FISMA reporting requirements established by the Department of Homeland Security.

70. The purpose of the IG's audit function is to evaluate and ensure OPM's compliance with the information security requirements of FISMA. Pursuant to FISMA, the IG is required to review several facets of OPM's information security program.

71. In each annual audit from 2011 to 2014, the IG found that OPM maintained an adequate capital planning and investment program for funding information security. In each of those years, however, the IG found that OPM had not fulfilled its information security obligations under federal law.

72. In the reporting of audit results, non-negligible security concerns of the IG are termed "significant deficiencies." More serious concerns that the IG determines pose an immediate risk to the security of assets or operations are termed "material weaknesses."

73. In each annual audit from 2007 to the present, the IG found that OPM's information security policies and practices suffered from material weaknesses.

74. Due to these material weaknesses and other information security deficiencies, OPM failed to comply with FISMA from 2007 to the present.

ii. Material Weaknesses Relating to Information Security Governance

75. OPM officials knew for several years before the OPM Breaches that OPM's information security governance and management protocols were not in compliance with FISMA. OPM officials knew for several years before the OPM Breaches that OPM's information security governance and management protocols contained material weaknesses that posed a significant threat to its systems. OPM failed to materially correct the deficiencies reported by the IG in these areas.

76. From 2007 to 2009, the IG found that OPM lacked required policies and procedures for managing information security. In 2009, the IG also found that, to the extent

information security policies and procedures did exist at OPM, they had not been tailored to OPM with appropriate procedures and implementing guidance.

77. In 2009, the IG expanded the material weakness rating to cover OPM's overall information security governance program and information security management structure. A Flash Audit Alert from the IG in May 2009 identified four primary deficiencies:

a. OPM misrepresented the status of its information security program;

b. OPM's security policies and procedures were severely outdated;

c. OPM's security program was understaffed; and

d. OPM had been operating for over 14 months without a senior information security official.

78. In the 2010 FISMA audit, the IG again found that OPM's information security governance constituted a material weakness. In the 2010 FISMA audit, the IG faulted OPM for failing to remedy or otherwise address most of the deficiencies found in the 2007, 2008, and 2009 audits. OPM's policies, according to the IG, failed to provide employees with adequate guidance to secure OPM's information systems. In response, OPM stated its intent to implement comprehensive information security and privacy changes in fiscal year 2011.

79. In the 2011 FISMA audit, the IG found that OPM still lacked necessary security policies and procedures, including for agency-wide risk management, monitoring of security controls, and oversight of systems operated by a contractor. OPM's security policies again were not tailored to OPM's systems and were unaccompanied by needed guidance. The IG determined that OPM lacked a centralized security structure. Officials at various OPM divisions were responsible for testing and maintaining their own information security measures, without the guidance or oversight of the Chief Information Officer. The IG advised OPM to centralize

its management structure to ensure coordinated implementation of needed information security upgrades. The IG also found that many of OPM's information security officers were not actually information security professionals. These officers had been tasked with security functions in addition to their other full-time roles at OPM. The IG reported that OPM still was not providing appropriate guidance to its employees concerning management of systems risks.

80. By 2012, OPM had begun hiring information security professionals and centralizing its information security management structure. Nevertheless, the IG maintained its material weakness rating in its 2012 audit. In that audit the IG stated that OPM had only hired enough information security professionals to manage about one-third of OPM's information systems and that the new professionals had not performed any tangible work.

81. OPM contested the 2012 material weakness rating on the grounds that it had not suffered any loss of financial or personal information. The IG rejected OPM's position, stating that OPM's systems had, in fact, been breached on numerous occasions, resulting in the loss of sensitive data.

82. In 2013, the IG reiterated its material weakness rating of OPM's information security governance. The IG also noted that, since its last audit, OPM had not hired more security officers, thereby failing to remedy or otherwise address a central IG concern from previous years.

83. The IG's 2014 audit found that OPM still lacked a centralized cybersecurity team of individuals responsible for overseeing all of OPM's cybersecurity efforts and that OPM remained non-compliant with many FISMA requirements. The IG upgraded OPM's information security governance program from a "material weakness" to a "significant deficiency" rating,

based on imminently planned improvements. The IG warned that it would reinstate the material weakness rating as to information security governance if the proposed changes were not made.

iii. Material Weaknesses Relating to Security Assessments and Authorizations of OPM Systems

84. FISMA requires OPM to certify that its information systems' technological security controls meet applicable requirements and to decide whether to authorize operation of an information system and accept the associated risk. FISMA's requirement that OPM certify and accredit system security controls is known as Security Assessment and Authorization.

85. The IG's 2010 FISMA audit found that OPM's process for certifying and accrediting system security controls was incomplete, inconsistent, of poor quality, and characterized by material weaknesses. The deficiencies stemmed in part from the fact that OPM's security officers lacked information security experience and training and were not subject to a centralized security management structure. Six OPM systems had expired authorizations in 2010, and another system had been in use for several years without being validly authorized.

86. In 2014, the IG reinstated the material weakness rating after having removed OPM's process for certifying and accrediting system security controls as a security concern in 2012 and 2013. Of the 21 OPM systems due to be authorized in 2014, eleven authorizations had not been completed. The IG recommended that OPM levy administrative sanctions on several OPM divisions, including Federal Investigative Services, whose systems were operating without valid authorizations.

87. The OPM systems operating without authorizations in 2014 included some of OPM's most critical and sensitive applications. One was a general system that supported and provided the electronic platform for approximately two-thirds of all information systems operated by OPM. Two other OPM systems operating without authorizations in 2014 were used

by OPM's Federal Investigative Services division. Weaknesses in the information systems of this division, the IG warned OPM, raised national security implications.

88. The IG determined in 2014 that the lack of valid authorizations of OPM's systems was a critical and time-sensitive problem. The IG found OPM had failed to ensure that the security controls for its systems were working. The IG also found OPM lacked a way to monitor these systems for cyberattacks or data breaches. Based on these findings, the IG advised OPM to shut down all systems lacking a current and valid authorization. The IG's advice was unprecedented.

89. OPM chose not to follow the IG's 2014 recommendation to shut down the unauthorized systems.

iv. Other Deficiencies in OPM's Security Controls

90. OPM officials were aware of several other information security deficiencies summarized below. The deficiencies summarized below existed within OPM's systems immediately prior to the OPM Breaches. Each was identified and described in IG audits.

91. OPM failed to implement or enforce multi-factor authentication. OPM's failure to implement or enforce multi-factor identification increased the risk of a breach of OPM's information systems. Multi-factor authentication improves data security because a user needs more than one form of credential to access software systems. For example, the user inputs a password and also scans a PIV card with an embedded microchip. In 2011, Homeland Security Presidential Directive 12 and OMB Memorandum M-11-11 became binding on OPM. Homeland Security Presidential Directive 12 and OMB Memorandum M-11-11 require OPM to implement multi-factor authentication with PIV for its information systems. Immediately prior to the OPM Breaches, none of OPM's major information systems required PIV authentication.

92. OPM failed to promptly patch or install security updates for its systems. OPM's failure to patch or install security updates increased the vulnerability of OPM's systems to breach.

93. OPM lacked a mature vulnerability scanning program to find and track the status of security weaknesses in its systems. OPM lacked a centralized network security operations center to continuously monitor security events, and failed to continuously monitor the security controls of its software systems.

94. When employees accessed OPM's systems from a remote location, the remote access sessions did not terminate or lock out as required by FISMA. As a result, connections to OPM's systems were left open and vulnerable.

95. OPM lacked the ability to detect unauthorized devices connected to its network.

96. OPM failed to engage in appropriate oversight of its contractor-operated systems.

97. OPM failed to comply with several standards to which FISMA requires it to adhere, including in the areas of risk management, configuration management, incident response and reporting, continuous monitoring management, and contingency planning. 40 U.S.C. § 11331.

98. Only 37 of OPM's 47 software systems had been adequately tested for security in 2014, and it had been over eight years since all systems were tested.

C. Cyber Attackers Breach the Systems of OPM's Contractors

99. In or around December 2013, cyber attackers breached the information systems of Peraton and U.S. Investigations Services ("USIS") without being detected. At the time, Peraton and USIS were the primary contractors responsible for conducting the fieldwork for OPM's background and security clearance investigations.

100. In June 2014, USIS detected a breach of its systems and informed OPM that thousands of government employees' personal information might have been compromised. USIS ultimately sent out 31,000 notices of this data breach to federal employees.

101. Following the USIS breach, OPM rescinded its contracts with USIS. At the time, USIS was performing approximately 21,000 background checks per month. Peraton doubled the size of its work force to staff its additional responsibilities. Peraton failed to concurrently increase managerial oversight given its increased staff and additional responsibilities.

102. The December 2013 Peraton Breach was detected in September 2014. The nature and scope of the Peraton Breach indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive data for improper use.

103. Following the disclosure of the Peraton Breach, the United States Customs Service and Border Protection suspended all investigations being conducted on its behalf by Peraton until Peraton took steps to protect GII in and connected to Peraton's systems.

104. OPM did not suspend Peraton's investigations, rescind its contract with Peraton, prevent or limit Peraton's access to OPM systems, or take any measure adequate to mitigate the potential adverse effects of the Peraton Breach.

105. On April 27, 2015, OPM alerted more than 48,000 federal employees that their personal information might have been exposed in the Peraton Breach.

106. Peraton lacked software logs to track malware entering its systems and data exiting its systems. Precisely how the Peraton Breach occurred has not been disclosed.

107. By unreasonably failing to safeguard its security credentials and Plaintiffs' and Class Members' GII, Peraton departed from its mandate, exceeded its authority, and breached its contract with OPM.

108. The contract between OPM and Peraton incorporates the requirements of the Privacy Act. 5 U.S.C. § 552a(m)(1). Peraton violated the Privacy Act and breached its contract with OPM by failing to ensure the security and confidentiality of records and to protect against known and anticipated threats or hazards to their security or integrity which could cause substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class Members. Peraton also violated the Privacy Act and breached its contract with OPM by disclosing Plaintiffs' and Class Members' records without their prior written consent for no statutorily permitted purpose.

109. In addition to departing from the commands and directives of federal law, Peraton acted negligently in performing its obligations under its contract with OPM.

D. Cyber Attackers Breach OPM's Systems

i. The Information Technology Documents Breach (November 2013)

110. On November 1, 2013, OPM's network was infiltrated. No GII was stolen. The hackers stole security system documents and electronic manuals concerning OPM's information technology assets. The stolen information provided a blueprint to OPM's network.

111. When OPM later announced this breach to the public, OPM disclosed only that no GII had been compromised; it did not disclose the theft of its security system documents and information technology manuals.

ii. The Background Investigation Breach (May 2014)

112. On May 7, 2014, hackers accessed OPM's network using stolen Peraton credentials. Once inside OPM's network, they installed malware and created a conduit through which data could be exfiltrated.

113. The nature and scope of the May 2014 breach indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive information for improper use.

114. The May 2014 breach was not detected for almost a year. It resulted in the theft of nearly 21.5 million background investigation records, including many million questionnaire forms containing highly sensitive personal, family, financial, medical, and associational information of Class Members.

115. The two primary systems the hackers targeted, and from which they removed data, were (i) the Electronic Official Personnel Folder system, and (ii) the database associated with the EPIC software used by the Federal Investigative Services office to collect information for government employee and contractor background checks.

iii. The Personnel Records Breach (October 2014)

116. No later than October 2014, hackers launched another successful cyberattack against OPM systems maintained in an Interior Department shared-services data center. The October 2014 breach resulted in the loss of approximately 4.2 million federal employees' personnel files.

117. The nature and scope of the October 2014 breach indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive data for improper use.

118. Because OPM's systems were not shielded through multi-factor authentication or privileged access controls, the hackers were able to use the stolen Peraton credentials to access systems within OPM's network at will. During the several months in which the intruders maintained such access, they removed millions of personnel records via the Internet, hidden among normal traffic.

E. Causes of the OPM Breaches

119. Millions of unauthorized attempts to access sensitive United States government data systems take place each month. OPM's prioritization of accessibility and convenience over security foreseeably heightened the risk of a successful intrusion into OPM's systems. OPM's

decisions not to comply with FISMA requirements for critical security safeguards enabled hackers to access and loot OPM's systems for nearly a year without being detected.

120. OPM's inadequate patching of software systems contributed to the OPM Breaches. When a security flaw in a software system is discovered, the developer of that system often will create and recommend installing an update—or "patch"—to eliminate that vulnerability. Failure to promptly install such a patch exposes a software system to known and preventable risks. In multiple FISMA audits, the IG found that OPM was not adequately patching its software systems and that its failure to do so represented an information security deficiency.

121. Other known deficiencies that contributed to the OPM Breaches include OPM's failures to establish a centralized management structure for information security, to encrypt data at rest and in transit, and to investigate outbound network traffic that did not conform to the Domain Name System ("DNS") Protocol.

122. Additionally, OPM's sub-networks were not segmented through the use of privileged access controls or multi-factor authentication. OPM's failure to implement such tiered identity management controls for system administrators exposed hundreds of its sub-networks, instead of a single sub-network, to breach. Had OPM implemented such controls, as required by OMB Memorandum M-11-11, the intrusion would have been detected earlier and the cyber thieves prevented from accessing the entire OPM network.

F. Announcements of the OPM Breaches

123. On June 4, 2015, OPM announced the October 2014 breach. OPM disclosed that the breach had resulted in the exposure and theft of the GII of approximately 4.2 million current, former, and prospective federal employees and contractors.

124. On June 12, 2015, OPM announced that the scope of the incident was broader than it had initially disclosed and that the GII of as many as 14 million current, former, and prospective federal employees and contractors had likely been exposed and stolen.

125. On July 9, 2015, OPM announced that the GII of approximately 21.5 million people had been exposed and stolen in the May 2014 breach. OPM disclosed that, of these compromised records, 19.7 million concerned individuals who had undergone federal background checks. OPM also disclosed that some of these records contained findings from interviews conducted by background investigators, as well as approximately 1.1 million fingerprints. OPM stated that the remaining 1.8 million compromised records concerned other individuals: mostly job applicants' spouses, children, and other cohabitants.

126. On September 23, 2015, OPM announced that it had underestimated the number of compromised fingerprints, and that approximately 5.6 million fingerprints had been exposed and stolen in the cyberattacks on its systems.

127. Prior to OPM's announcements of the Data Breaches, Plaintiffs and Class Members lacked notice that their GII might have been the subject of an unauthorized disclosure. Prior to these announcements, Plaintiffs and Class Members did not have a reasonable basis to suspect or believe that such an unauthorized disclosure had occurred. Plaintiffs and Class Members only learned that their GII had in fact been compromised when they subsequently received written notification from OPM.

G. What the Compromised Records Contain

128. The records taken in the Data Breaches are of the utmost sensitivity. Their theft violates the privacy rights and compromises the safety of tens of thousands of individuals, including covert intelligence agents.

129. Highly sensitive personal information was exposed and stolen in the Data Breaches. Among the compromised information:

- Residency details and contact information;
- Marital status and marital history;
- Private information about children, other immediate family members, and relatives;
- Information about financial accounts, debts, bankruptcy filings, and credit ratings and reports;
- Identities of past sexual partners;
- Findings from interviews conducted by background check investigators;
- Character and conduct of individuals as reported by references;
- Social Security numbers and birthdates of applicants and their spouses, children, and other cohabitants;
- Educational and employment history;
- Selective service and military records;
- Identities of personal and business acquaintances;
- Foreign contacts, including with officials and agents of foreign governments;
- Foreign travel and activities;
- Passport information;
- Psychological and emotional health information;
- Responses to inquiries concerning gambling compulsions, marital troubles, and past illicit drug and alcohol use;
- Police and arrest records;

- Association records;
- Investigations and clearance records;
- Information relating to criminal and non-criminal legal proceedings; and
- Financial and investment records.

130. The Electronic Official Personnel Folders stolen in the OPM Breaches include employee performance records, employment history, employment benefits information, federal job applications, resumes, school transcripts, documentation of military service, and birth certificates.

131. Stolen federal job applications and investigation forms contain, among other information, Social Security numbers, birthdates, birthplaces, other names used, mailing addresses, and financial records that include bank account and credit card information.

132. Also stolen was so-called adjudication information that federal investigators gather on those who apply for positions requiring heightened security clearance, such as positions in intelligence services. Adjudication information includes the results of polygraph examinations and the details of previous confidential work, as well as intimate personal facts. Exposure of this information imperils the safety of those who work covertly to protect American interests around the world.

H. OPM Remedial Measures

133. Following the Data Breaches, OPM notified people whose GII was compromised and offered them free identity theft protection services for a limited period of time. Specifically, OPM emailed federal employees whose GII was compromised, offering identity theft protection services via a link in the email. After some federal employees received unauthorized duplicates

of these notification emails with false links that asked them to divulge personal information, OPM stopped sending notifications by email, and began sending paper notifications in the mail.

134. OPM hired CSID and ID Experts—companies specializing in fraud resolution and identity theft protection—to provide services to individuals affected by the OPM Breaches.

135. At a combined cost of approximately $154 million, these companies agreed to provide victims with fraud monitoring and identity theft protection, insurance, and restoration services for either 18 months or three years, depending on the amount and sensitivity of the compromised GII.

136. Congress subsequently authorized "complimentary identity protection coverage"—including "not less than $5,000,000 in identity theft insurance"—for all individuals whose personal information was compromised in the Data Breaches, through September 2026. (Consolidated Appropriations Act of 2017, Pub. L. 115-31, tit. VI, sec. 633 (May 5, 2017).) OPM contracted with ID Experts—now known as IDX—which has been providing such individuals a free set of credit monitoring, identity theft protection services, and data theft insurance products known as MyIDCare. Approximately 3.2 million victims of the Data Breaches have signed up for MyIDCare.

137. OPM refers victims who wish to receive additional protection to identitytheft.gov, a website managed by the FTC. That website recommends that individuals with compromised Social Security numbers purchase a credit freeze to ensure that no one can pull or modify a credit report. A credit freeze typically costs between $5 and $15. This remedial option is not included in the package being offered by OPM.

V. PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

138. As a result of Defendants' violations of law, Plaintiffs and Class Members have sustained and will continue to sustain economic loss and other harm. They have experienced and/or face an increased risk of experiencing the following forms of injuries:

A. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and other unauthorized uses of GII, including by identifying, disputing, and seeking reimbursement for fraudulent activity and canceling compromised financial accounts and associated payment cards;

B. money and time lost as a result of fraudulent access to and use of their financial accounts, some of which accounts were never reimbursed;

C. loss of use of and access to their financial accounts and/or credit;

D. diminished prospects for future employment and/or promotion to positions with higher security clearances as a result of their GII having been compromised;

E. money and time expended to order credit reports and place temporary freezes on credit, and to investigate options for credit monitoring and identity theft protection services;

F. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

G. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

H. money and time expended to ameliorate the consequences of the filing of fraudulent income tax returns, including by completing paperwork

associated with the reporting of fraudulent returns and the manual filing of replacement returns;

I. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breaches, including efforts to research how to prevent, detect, contest, and recover from misuse of GII;

J. anticipated future costs from the purchase of credit monitoring and identity theft protection services once the temporary services being offered by OPM expire;

K. loss of the opportunity to control how their GII is used;

L. continuing risks from the unmasking of confidential identities; and

M. continuing risks to their GII and that of their family members, friends, and associates, which remains subject to further harmful exposure and theft as long as OPM fails to undertake appropriate, legally required steps to protect the GII in its possession.

VI. CLASS ACTION ALLEGATIONS

139. Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed Class, pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3). This action satisfies the numerosity, commonality, typicality, predominance, and superiority requirements.

140. The proposed Class is defined as:

> All U.S. citizens and permanent residents whose personal information was compromised as a result of the breaches of the U.S. Office of Personnel Management's electronic information systems in 2014 and 2015 or the breach of Peraton's electronic information systems in 2013 and 2014, and who, after May 7, 2014, suffered out-of-pocket expense or loss of compensable time: (1) to purchase a credit monitoring product, credit or

> identity theft protection product, or other product or service designed to identify or remediate the data breaches at issue in this case; (2) to access, freeze, or unfreeze a credit report with a credit reporting agency; or (3) as a result of an identity theft incident or to mitigate an identity theft incident.
>
> Excluded from the Class are: Class Counsel and their employees; any judicial officers to whom this case is assigned and their respective staffs; mediators and their respective staffs; and attorneys from the Department of Justice and the U.S. Office of Personnel Management, and their respective staffs, who worked directly and personally on this matter.

Numerosity

141. The number of Class Members is so numerous that joinder of all members is impracticable. The Data Breaches compromised the personal information of approximately 22 million individuals; a reasonable inference thus arises that the Class includes at least thousands of members.

Typicality

142. Plaintiffs' claims are typical of the claims of the Class in that the sensitive personal information of the representative Plaintiffs, like that of all Class Members, was compromised in the Data Breaches.

Adequacy of Representation

143. Plaintiffs are members of the proposed Class and will fairly and adequately represent and protect its interests. Plaintiffs' counsel are competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiffs have no interests contrary to or in conflict with the interests of Class Members.

Predominance of Common Issues

144. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual Class Members. Among the questions of law and fact common to the Class are:

(a) Whether OPM, in violation of the Privacy Act, failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against anticipated threats to their security and integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class Members;

(b) Whether OPM, in violation of the Privacy Act, disclosed Plaintiffs' and Class Members' GII without their prior written consent for no statutorily permitted purpose;

(c) Whether OPM's decisions not to follow the IG's directions concerning FISMA requirements for information security constitute intentional or willful violations;

(d) Whether Peraton owed, and breached, duties to Plaintiffs and Class Members to implement reasonable and adequate cybersecurity measures and to promptly alert them if their GII was compromised;

(e) Whether Peraton acted negligently in failing to disclose, and falsely representing, material facts relating to its cybersecurity precautions;

(f) Whether Peraton engaged in unfair or deceptive acts or practices in the course of its business; and

(g) Whether Plaintiffs and Class Members are entitled to damages or restitution.

Superiority

145. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Absent a class action, most Class Members would likely find the cost of litigating their claims prohibitively high and would have no effective remedy. Because of the relatively small size of the individual Class Members' claims, it is likely that few, if any, Class Members could afford to seek redress for Defendants' violations.

146. Class treatment of common questions of law and fact also is a superior method to piecemeal litigation in that class treatment will conserve the resources of the courts and will promote consistency and efficiency of adjudication.

VII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
(Against OPM)
Violations of the Privacy Act of 1974, 5 U.S.C. § 552a

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

148. OPM is an agency within the meaning of the Privacy Act.

149. OPM obtained and preserved Plaintiffs' and Class Members' GII, including GII contained in SF-85, SF-85P, and SF-86 forms, in a system of records.

150. In violation of the Privacy Act, OPM willfully and intentionally failed to comply with FISMA. OPM's violations of federal law adversely affected Plaintiffs and Class Members. Despite known and persistent threats from cyberattacks, OPM allowed multiple "material weaknesses" in its information security systems to continue unabated. As a result, Plaintiffs' and Class Members' GII under OPM's control was exposed, stolen, and misused.

151. IG reports repeatedly warned OPM officials that OPM's systems were highly vulnerable to cyberattacks and not in compliance, in several specific ways, with the Privacy Act, FISMA, and other rules and regulations governing cybersecurity at OPM. OPM officials knew that these warnings were well-founded: among other things, OPM suffered successful cyberattacks in 2009 and 2012. OPM officials were also aware that each month saw more than 10 million attempted electronic incursions against its information systems. OPM officials, however, decided not to take adequate, legally required measures to protect the data with which the agency had been entrusted.

152. OPM was required—but failed—to take many steps to comply with controlling information security rules and regulations. OPM declined to implement PIV multi-factor authentication for all 47 of its major applications, as required by OMB Memorandum M-11-11 and as stated in the IG's audit reports. OPM affirmatively refused to shut down faulty systems even after the IG notified OPM that it was required to do so under FISMA. OPM's violations of applicable federal law include its willful failures to ensure that all operating software systems receive valid authorizations; to centralize its cybersecurity structure to provide effective management of its information systems; to monitor those systems continuously and create internal firewalls to limit the adverse effects of a breach; and to adequately train its employees responsible for cybersecurity. OPM intentionally disregarded IG findings that each of these failures rendered the agency not in compliance with federal requirements.

153. In violation of the Privacy Act and FISMA, OPM intentionally failed to comply with many other standards promulgated under 40 U.S.C. § 11331, including with regard to risk and configuration management, incident response and reporting, contractor systems, security capital planning, and contingency planning. OPM's actions were calculated to downplay the

scope of the OPM Breaches and to preserve data accessibility to the detriment of data confidentiality and integrity. OPM did not destroy GII where permitted, and allowed GII to be accessible to unauthorized third parties.

154. In a continuous course of wrongful conduct, OPM willfully refused to implement electronic security safeguards required by law. OPM willfully failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could cause substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class Members, in violation of 5 U.S.C. § 552a(e)(10).

155. As a direct and proximate result of its non-compliance with federal requirements and its intentional disregard of the IG's findings under FISMA, OPM willfully disclosed Plaintiffs' and Class Members' records without their prior written consent for no statutorily permitted purpose, in violation of 5 U.S.C. § 552a(b).

156. Plaintiffs and Class Members have sustained actual damages and pecuniary losses directly traceable to OPM's violations set forth above. Plaintiffs and Class Members are therefore entitled to damages under 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

SECOND CLAIM FOR RELIEF
(Against Peraton)

Negligence

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

158. It was reasonably foreseeable to Peraton that a breach of its information systems could occur and cause harm by compromising the GII of current, former, and prospective federal government employees. Peraton's and OPM's electronic systems were linked, shared, and

overlapping. It was reasonably foreseeable that a breach of Peraton's systems would expose OPM's systems, and the GII contained therein, to a successful cyberattack.

159. Peraton owed a duty of care to Plaintiffs and Class Members to adequately protect their GII—both in Peraton's network and in OPM's network—and the security credentials that could be used to access that GII. More specifically, with regard to Plaintiffs and Class Members, Peraton was obligated to:

a. exercise due and reasonable care in obtaining, retaining, securing, protecting, and deleting GII in Peraton's possession;

b. exercise due and reasonable care in providing, securing, protecting, and deleting the security credentials for accessing GII on Peraton's and OPM's systems;

c. exercise due and reasonable care in expanding its workforce by, among other things, performing due diligence of candidates who, if hired, would have access to GII and appropriately supervising new hires;

d. safeguard GII through security procedures, protocols, and systems that are reasonable, adequate, and in conformance with recognized data security industry standards; and

e. implement procedures and protocols to promptly detect, record, mitigate, and notify the victims of data breaches.

160. Peraton's duties in these respects applied to Plaintiffs and Class Members because they were the reasonably foreseeable victims of breaches of its information systems. Peraton collected and stored Plaintiffs' and Class Members' GII in the course of conducting background and security clearance investigations. Peraton knew or should have known of the risks inherent in collecting and storing GII and the crucial importance of adequate data security, including to protect the access credentials relied on to perpetrate the Data Breaches.

161. Peraton owed similar duties of care to Plaintiffs and Class Members under FCRA and state statutes requiring Peraton to reasonably safeguard Plaintiffs' and Class Members' GII and to promptly notify them of any breach thereof.

162. Peraton's duties of care also arose from the special relationship between Peraton and those who entrusted it with their sensitive personal information. Plaintiffs and Peraton Subclass members permitted Peraton to access such information with the expectation that Peraton would take reasonable and effective precautions to protect such information from disclosure to unauthorized third parties and/or for improper purposes.

163. Peraton knew or should have known that its information security defenses did not reasonably or effectively protect Plaintiffs' and Class Members' GII and the credentials used to access it on Peraton's and OPM's systems. Peraton's information security defenses did not conform to recognized industry standards.

164. Peraton's acts and omissions created a foreseeable risk of harm to Plaintiffs and Class Members, breaching the duties of care it owed them. Peraton's breached its duties by failing to:

a. secure its systems for gathering and storing GII, despite knowing of their vulnerabilities;

b. comply with industry-standard data security practices;

c. perform requisite due diligence and supervision in expanding its workforce;

d. encrypt GII at collection, at rest, and in transit;

e. employ adequate network segmentation and layering;

f. ensure continuous system and event monitoring and recording; and

g. otherwise implement security policies and practices sufficient to protect Plaintiffs' and Class Members' GII from unauthorized disclosure.

165. Peraton also breached its duties to Plaintiffs and Class Members by failing to cause them to be promptly notified that their GII had been compromised. The Peraton Breach occurred in December 2013, was detected in September 2014, and was disclosed to the public on April 27, 2015.

166. But for Peraton's wrongful and negligent breaches of its duties of care, Plaintiffs' and Class Members' GII would not have been compromised or they would have mitigated their damages more effectively.

167. Had Peraton promptly caused Plaintiffs and Class Members to be notified of the breach of its information systems, they could have avoided or more effectively mitigated the resulting harm. They could have placed freezes and/or fraud alerts on their credit, cancelled compromised accounts, and promptly taken other security precautions to prevent or minimize the adverse consequences of GII misuse. Additionally, those whom Peraton began to investigate after its systems had been breached could have declined to provide their sensitive personal information to Peraton.

168. Plaintiffs and Class Members sustained harm as a result of Peraton's negligence in failing to prevent and to timely cause them to be notified of the Peraton Breach.

169. Plaintiffs and Class Members sustained harm as a result of Peraton's negligence in failing to protect and secure its user log-in credentials. Peraton's negligence in failing to protect and secure its user log-in credentials was a substantial factor in causing the Data Breaches.

170. Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

THIRD CLAIM FOR RELIEF
(Against Peraton)
Violations of State Statutes Prohibiting Unfair and Deceptive Trade Practices

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

172. Peraton is engaged in trade and commerce. As relevant here, Peraton's acts, practices, and omissions occurred in the course of Peraton's business of conducting background and security clearance investigations of Plaintiffs and Class Members throughout the United States.

173. Peraton's conduct as alleged herein constitutes unfair, deceptive, fraudulent, unconscionable, and/or unlawful acts or practices. Among other violations, Peraton:

a. failed to implement and maintain data security practices adequate to safeguard Plaintiffs' and Class Members' GII and the security credentials used to breach its and OPM's information systems;

b. made misleading and deceptive representations and omissions in its publicly disseminated Privacy Policy regarding its ability and efforts to secure Plaintiffs' and Class Members' GII;

c. failed to disclose that its data security practices and protocols were insufficient to protect Plaintiffs' and Class Members' GII;

d. failed to timely disclose the Peraton Breach to Plaintiffs and Class Members; and

e. continued to accept and store Plaintiffs' and Class Members' GII even after obtaining actual or constructive notice of its security vulnerabilities.

174. By reason of its acts and omissions, Peraton violated the following statutes prohibiting unfair or deceptive acts or practices:

a. The California Unfair Competition Law, Cal. Bus. & Prof. Code, § 17200, *et seq.*;

b. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq.*;

c. The Idaho Consumer Protection Act, Idaho Code Ann. § 48-603(18), *et seq.*;

d. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 505/2, *et seq.*, and the Illinois Uniform Deceptive Trades Practices Act, 815 Ill. Comp. Stat. § 510/2(a)(12), *et seq.*;

e. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915, *et seq.*;

f. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(17) & 57-12-3, *et seq.*;

g. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(14), *et seq.*; and

h. The Washington Consumer Protection Act, Wash. Rev. Code Ann. § 19.86.020, *et seq.*

175. As a direct and proximate result of Peraton's violations of the above provisions, Plaintiffs and Class Members sustained damages, as described herein, and are entitled to

appropriate monetary and equitable relief as well as attorneys' fees and costs as may be permitted by statute.

176. Before filing this Complaint, counsel for Plaintiffs sent a copy of this Complaint to the Attorney General of Washington, pursuant to Wash. Rev. Code § 19.86.095.

FOURTH CLAIM FOR RELIEF
(Against Peraton)
Violations of State Data Breach Acts

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

178. The Peraton Breach constitutes a security breach that triggered the requirements of various state data breach acts. The GII exposed and stolen in the Peraton Breach includes personal information protected by these statutes.

179. In violation of state data breach acts, Peraton unreasonably delayed in causing Plaintiffs and Class Members to be notified of the Peraton Breach after Peraton knew or should have known of it. The Peraton Breach occurred in December 2013, was detected in September 2014, and was disclosed to the public on April 27, 2015.

180. Peraton's failure to cause timely notice of the Peraton Breach to be provided violated the following statutes:

a. Cal. Civ. Code § 1798.80, *et seq.*;

b. 815 Ill. Comp. Stat. 530/10(a), *et seq.*;

c. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

d. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

e. Va. Code Ann. § 18.2-186.6(B), *et seq.*;

f. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*; and

g. Wis. Stat. Ann. § 134.98(2), *et seq.*

181. Peraton's violations of these statutes damaged Plaintiffs and Class Members. Had Peraton timely caused Plaintiffs and Class Members to be notified of the breach of its information systems, they could have avoided or more effectively mitigated the resulting harm. They could have placed freezes and/or fraud alerts on their credit, cancelled compromised accounts, and promptly taken other security precautions to prevent or minimize the adverse consequences of misuse of their sensitive personal information. Additionally, those whom Peraton began to investigate after its systems had been breached could have declined to provide their sensitive personal information to Peraton.

182. In further violation of Cal. Civ. Code § 1798.80, *et seq.*, Peraton failed to implement and maintain security measures sufficient to prevent the Peraton Breach and protect the security credentials used to perpetrate the Data Breaches. Peraton's violations of Cal. Civ. Code § 1798.80 damaged Plaintiffs and Class Members.

183. Peraton failed to establish appropriate procedures to ensure the confidentiality of Plaintiffs' and Class Members' medical information and to protect such information from unauthorized use and disclosure, in violation of Cal. Civ. Code § 56.20-56.245, *et seq.* Peraton also violated Wis. Stat. §§ 146.82 and 146.84 and Va. Code § 32.1-127.1:03(3) by disclosing Plaintiffs' and Class Members' medical records without specific authorization or other justification. Peraton's violations of Cal. Civ. Code § 56.20-56.245, *et seq.*, Wis. Stat. §§ 146.82 and 146.84, and Va. Code § 32.1-127.1:03(3) damaged Plaintiffs and Class Members.

184. Based on Peraton's violations of the foregoing provisions, Plaintiffs and Class Members are entitled to appropriate monetary and equitable relief as well as attorneys' fees and costs as may be permitted by statute.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs seek a judgment against Defendants through an Order:

A. certifying this case as a class action, designating Plaintiffs as Class and Subclass representatives, and appointing Plaintiffs' counsel to represent the Class;

B. finding Defendants liable for their failure to establish adequate and legally required safeguards to ensure the security of Plaintiffs' and Class Members' GII compromised in the Data Breaches;

C. requiring Defendants to pay money damages, including actual and statutory damages, or restitution to Plaintiffs and Class Members;

D. awarding reasonable attorneys' fees and costs as may be permitted by law;

E. awarding pre-judgment and post-judgment interest as may be prescribed by law; and

F. granting such further and other relief as may be just and proper.

IX. JURY TRIAL DEMANDED

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

DATED: May 6, 2022

Respectfully submitted,

GIRARD SHARP LLP

/s/ *Daniel C. Girard*
Daniel C. Girard
Jordan Elias
Simon S. Grille
601 California Street
Suite 1400
San Francisco, CA 94108
(415) 981-4800
dgirard@girardsharp.com

Interim Lead Class Counsel

David H. Thompson
Peter A. Patterson
COOPER & KIRK, PLLC
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036

Tina Wolfson
AHDOOT & WOLFSON, PC
2600 West Olive Avenue
Suite 500
Burbank, CA 91505

John Yanchunis
Marcio W. Valladares
Patrick A. Barthle II
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street
7th Floor
Tampa, FL 33602

Plaintiffs' Steering Committee

Gary E. Mason
MASON LIETZ & KLINGER LLP
5101 Wisconsin Avenue, N.W.
Suite 305
Washington, D.C. 20016

Liaison Counsel

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road
Suite 200
Kansas City, MO 64112

Additional Plaintiffs' Counsel