UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

STEVEN FOWLER, individually and on behalf of all others similarly situated, Plaintiff, v. CANON BUSINESS PROCESS SERVICES, INC. and GENERAL ELECTRIC COMPANY, Defendants.	**CASE NO.** **CLASS ACTION COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORY AND INJUNCTIVE RELIEF** **JURY DEMAND**

CLASS ACTION COMPLAINT

1. Plaintiff, STEVEN FOWLER, individually and on behalf of all others similarly situated, brings this action against Defendants CANON BUSINESS PROCESS SERVICES, INC. ("Canon") and GENERAL ELECTRIC COMPANY ("GE") (collectively, "Defendants") to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendants. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

JURISDICTION AND VENUE

2. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. Upon information and belief, the number of class members is in the hundreds of thousands, many of whom have different citizenship from Defendants, including the named Plaintiff here.

3. This Court has jurisdiction over the Defendants that operate and/or are incorporated in this District, and the computer systems implicated in this Data Breach are likely based in this District.

4. Through their business operations in this District, Defendants intentionally avail themselves of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

5. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Canon, GE's agent and service provider, is based in this District, maintains employees' personally identifiable information ("PII") in the District and has caused harm to Class Members residing in this District.

NATURE OF THE ACTION

6. This class action arises out of the recent data breach that was perpetrated against Defendant Canon, which held in its possession PII of Defendant GE's employees, former employees, and other beneficiaries entitled to benefits from GE (the "Data Breach").

7. The PII exposed in the Data Breach included, among other things: direct deposit forms, driver's licenses, passports, birth certificates, marriage certificates, death certificates, medical child support orders, tax withholding forms, beneficiary designation forms and applications for benefits such as retirement, severance and death benefits with related forms and documents, may have included names, addresses, Social Security numbers, driver's license numbers, bank account numbers, passport numbers, dates of birth, and other information contained in the relevant forms.

8. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect employees' and former employees' (and their beneficiaries') PII.

9. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' PII that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

10. Defendants maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant Canon's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiff's and Class Members' PII was a known risk to Defendants, and thus Defendants were on notice that failing to take steps necessary to secure the PII from those risks left that property in a dangerous condition.

11. Defendants disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Class Member PII; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members prompt and accurate notice of the Data Breach.

12. In addition, Defendant Canon (acting in the course and scope of its agency relationship with Defendant GE) and its employees failed to properly monitor the computer

network and systems that housed the PII. Had Canon properly monitored its property, it would have discovered the intrusion sooner.

13. Plaintiff's and Class Members' identities are now at risk because of Defendants' negligent conduct since the PII that Defendant GE collected and maintained through its agent, Canon, is now in the hands of data thieves.

14. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

15. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

16. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

17. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

18. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

19. Accordingly, Plaintiff brings this action against Defendants seeking redress for their unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of express contract, (iv) breach of implied contract, (v) breach of fiduciary duty and, (vi) violation of New York General Business Law Section 349.

STATEMENT OF FACTS

A. The Data Breach

20. In February of 2020, GE was informed that one of its service providers, Canon, experienced a data security incident.

21. GE contracts with Canon to process documents of GE employees, former employees and beneficiaries entitled to benefits. Pursuant to that contract, Canon acts as GE's authorized agent for processing and storage of certain documents of GE employees, former employees, and beneficiaries entitled to benefits.

22. GE learned that, between approximately February 3 - 14, 2020, an unauthorized party gained access to an email account that contained documents of certain GE employees, former employees and beneficiaries entitled to benefits that were maintained on Canon's systems

23. Canon informed GE that the affected documents, which contained certain PII, were uploaded by or for GE employees, former employees and beneficiaries entitled to benefits in connection with Canon's workflow routing service.

24. The data consisted of a wealth of GE employees', former employees' and beneficiaries' PII such as direct deposit forms, driver's licenses, passports, birth certificates, marriage certificates, death certificates, medical child support orders, tax withholding forms, beneficiary designation forms and applications for benefits such as retirement, severance and death benefits with related forms and documents, and may have included names, addresses, Social

Security numbers, driver's license numbers, bank account numbers, passport numbers, dates of birth, and other information contained in the relevant forms.

25. Internet security specialists recognized that the PII leaked in the Data Breach presents "a treasure trove" of information which could be sold on underground forums to other criminals and fraudsters, or used to target individuals with convincing scam emails and phishing attacks.[1]

26. "While I'm usually a bit numb to the latest data breach, the sheer variety of exposed information is unique," said cybersecurity expert Roger Grimes, of the Data Breach.[2]

27. On or about February 28, 2020, GE notified affected consumers and various governmental agencies of the Data Breach. The Notice of Data Incident ("Notice") stated in relevant part the following:

Notice of Data Incident

What Happened
We were notified on February 28, 2020 that Canon had determined that, between approximately February 3 - 14, 2020, an unauthorized party gained access to an email account that contained documents of certain GE employees, former employees and beneficiaries entitled to benefits that were maintained on Canon's systems.

What Information Was Involved
Canon has indicated that the affected documents, which contained certain personal information, were uploaded by or for GE employees, former employees and beneficiaries entitled to benefits in connection with Canon's workflow routing service. The relevant personal information, which was contained in documents such as direct deposit forms, driver's licenses, passports, birth certificates, marriage certificates, death certificates, medical child support orders, tax withholding forms, beneficiary designation forms and applications for benefits such as retirement, severance and death benefits with related forms and documents, may have included names, addresses, Social Security numbers, driver's license numbers, bank account numbers, passport numbers, dates of birth, and other information contained in the relevant forms.

[1] https://www.tripwire.com/state-of-security/featured/ge-data-breach-third-party/.
[2] https://www.scmagazine.com/home/security-news/phishing/canon-breach-exposes-personal-data-of-current-former-ge-employees-beneficiaries/.

What We Are Doing
After learning of the issue, we quickly began working with Canon to identify the affected GE employees, former employees and beneficiaries. We understand that Canon took steps to secure its systems and determine the nature of the issue. Canon also retained a data security expert to conduct a forensic investigation. GE systems, including your personal information in our systems, have not been affected by the Canon data security incident. We will work hard to understand how the unauthorized individual was able to access Canon's systems. We are taking steps to help ensure appropriate measures are implemented to prevent a reoccurrence of this kind of incident.

What You Can Do
We take our obligation to safeguard personal information very seriously and are alerting you about this issue so you can take steps to help protect yourself. You are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. We encourage you to remain vigilant by reviewing your account statements and monitoring your free credit reports. At our request, Canon is offering identity protection and credit monitoring services to affected individuals for two years at no cost to you through a company called Experian. The attached Reference Guide provides information on registration and the June 30, 2020 deadline to take advantage of these services.

B. GE Employment Data Protection Standards

28. GE has established Employment Data Protection Standards ("Privacy Policy") wherein it details the PII it collects from employees and its standards to maintain the security and integrity of such data.[3]

29. The aim of the Privacy Policy is to provide adequate and consistent safeguards for the handling of employment data by GE entities.

30. GE acknowledges the Privacy Policy covers job applicants, employees (whether temporary or permanent), contingent workers, retirees, and former employees, as well as any dependents or others whose personal data have been given to a GE entity by such persons.

[3] https://www.ge.com/content/dam/gepower-pw/global/en_US/documents/ec-supplier/GE_Employee_Data_Protection_Standards.pdf.

31. In its Privacy Policy, GE represents that it "respects the privacy rights and interests of each individual" and "GE entities will observe the following principles when processing Employment Data"

- Data will be processed fairly and lawfully.
- Data will be collected for specified, legitimate purposes and not processed further in ways incompatible with those purposes.
- Data will be relevant to and not excessive for the purposes for which they are collected and used. For example, data may be rendered anonymous when feasible and appropriate, depending on the nature of the data and the risks associated with the intended uses.
- Data will be accurate, and where necessary, kept up-to-date. Reasonable steps will be taken to rectify or delete Employment Data that is inaccurate or incomplete.
- Data will be kept only as long as it is necessary for the purposes for which it was collected and processed.
- Data will be processed in accordance with the individual's legal rights (as described in these Standards or as provided by law).
- Appropriate technical, physical, and organizational measures will be taken to prevent unauthorized access, unlawful processing, and unauthorized or accidental loss, destruction, or damage to data.

32. GE further represents and warrants in the Privacy Policy that "GE entities are committed to taking appropriate technical, physical, and organizational measures to protect Employment Data against unauthorized access, unlawful processing, accidental loss or damage, and unauthorized destruction."

33. GE represents and warrants that the following measures are taken to protect PII:

> **Equipment and Information Security**
> To safeguard against unauthorized access to Employment Data by third parties outside GE, all electronic Employment Data held by GE entities are maintained on systems that are protected by secure network architectures that contain firewalls and intrusion detection devices. The servers holding Employment Data are "backed up" (i.e., the data are recorded on separate media) on a regular basis to avoid the consequences of any inadvertent erasure or destruction of data. The servers are stored in facilities with comprehensive security and fire detection and response systems.
>
> **Access Security**
> GE entities limit access to internal systems that hold Employment Data to a select group of authorized users who are given access to such systems through the use of a unique identifier and password. Access to Employment Data is limited to and provided to individuals for the purpose of performing their job duties (e.g., a human resources manager may need access to an employee's compensation data to conduct salary planning, or a training manager may need to know the names of those who need certain training and the languages they speak). Decisions regarding such access are made by assigned security administrators. Compliance with these provisions will be required of third-party administrators who may access certain Employment Data, as described in Section IX. *TRANSFERRING DATA.*
>
> **Training**
> GE will conduct training regarding the lawful and intended purposes of processing Employment Data, the need to protect and keep information accurate and up-to-date, and the need to maintain the confidentiality of the data to which employees have access. Authorized users will comply with these Standards, and GE entities will take appropriate disciplinary actions, in accordance with applicable law, if Employment Data are accessed, processed, or used in any way that is inconsistent with the requirements of these Standards.

34. Although GE claims to employ industry standard security measures, this representation, along with the promise to maintain the integrity of consumers' PII was belied by its failure and the failure of its agent, Canon, to impose and maintain the necessary safeguards that would have prevented the Data Breach.

C. Prevalence of Cyber Attacks and Susceptibility of the Data Storage Industry

35. Data breaches have become widespread. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from

the previous year. In 2017, a new record high of 1,579 breaches were reported, representing a 44.7 percent increase over 2016. In 2018, there was an extreme jump of 126 percent in the number of consumer records exposed from data breaches. In 2019, there was a 17 percent increase in the number of breaches (1,473) over 2018, with 164,683,455 sensitive records exposed.[4]

36. What's more, companies in the business of storing and maintaining PII, such as Canon, are among the most targeted—and therefore at risk—for cyber-attacks.[5]

D. Defendants Acquire, Collect, and Store Plaintiff's and Class Members' PII

37. As its Privacy Policy makes clear, GE acquires, collects, and stores a massive amount of personally identifiable information ("PII") on its employees, former employees and beneficiaries.

38. As a condition of employment, or as a condition of receiving certain benefits, GE requires that its employees and their beneficiaries entrust it with highly sensitive personal information.

39. By obtaining, collecting, and using, Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

40. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

[4] https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/

[5] https://www.cshub.com/attacks/articles/top-8-industries-reporting-data-breaches-in-the-first-half-of-2019

41. Plaintiff and the Class Members relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

E. The Value of Personally Identifiable Information and the Effects of Unauthorized Disclosure

42. Defendants were well-aware that the PII GE collects is highly sensitive, and of significant value to those who would use it for wrongful purposes.

43. Personally identifiable information is a valuable commodity to identity thieves. As the FTC recognizes, with PII identity thieves can commit an array of crimes including identify theft, medical and financial fraud.[6] Indeed, a robust "cyber black market" exists in which criminals openly post stolen PII on multiple underground Internet websites.

44. The ramifications of Defendants' failure to keep Plaintiff's and Class Members' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

45. "And the problem is this. When your password gets compromised after a data breach, you can change your password. Of course it can be a pain and a nuisance to change your password, but it's not an insurmountable problem – and if you haven't made the mistake of reusing the same password in multiple places the impact of the breach is limited. ***But just try changing the details contained on your passport, your date of birth, your bank account details, or your social security number …*** GE says that, following the discovery of the breach, its partner Canon "took steps to secure its systems and determine the nature of the issue" and emphasizes that GE's

[6] Federal Trade Commission, *Warning Signs of Identity Theft,* https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft

own infrastructure was not compromised by the attackers. That's good, but it's not much consolation for the unknown number of past and present GE employees and their beneficiaries who have had their personal information fall into the hands of hackers."[7]

46. Similarly, cybersecurity expert Roger Grimes had this to say about the Data Breach: "Data in child support orders could lead an attacker to create a spear phishing email crafted with those specific details, pretending to be someone official claiming some impending event needs action right now or some unwelcome especially stressful event could occur … while knowledge of death certificates could help an attacker craft new synthetic identities based on details of that involved person to get new credit cards, loans, and other financial instruments."[8]

47. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences if its data security systems were breached, including, the significant costs that would be imposed on employees and their beneficiaries as a result of a breach.

48. Defendants breached their obligations to Plaintiff and Class Members and/or were otherwise negligent and reckless because they failed to properly maintain and safeguard the computer systems and data that held the stolen PII. Defendants' unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect consumers' PII;

[7] https://www.tripwire.com/state-of-security/featured/ge-data-breach-third-party/
[8] https://www.scmagazine.com/home/security-news/phishing/canon-breach-exposes-personal-data-of-current-former-ge-employees-beneficiaries/.

c. Failing to properly monitor the data security systems for existing intrusions, and;

d. Failing to ensure that its agents and service providers with access to Plaintiff's and Class Members' PII employed reasonable security procedures.

F. Defendants Failed to Comply with FTC Guidelines

49. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[9]

50. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses.[10] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

[9] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[10] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

51. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[11]

52. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

53. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to consumer PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

54. Defendants were at all times fully aware of their obligation to protect the PII of consumers. Defendants were also aware of the significant repercussions that would result from their failure to do so.

G. Defendants Fail to Comply with Industry Standards

55. Companies in the business of storing and maintaining PII, such as Canon, have been identified as being particularly vulnerable to cyber-attacks because of the value of the PII which

[11] Federal Trade Commission, *Start With Security*, available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

they maintain. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; and training staff regarding critical points.[12]

56. The Data Breach appears to have been caused by "a standard credential phishing attack or due to credential reuse on another site."[13]

57. Cybersecurity experts have explicitly noted that phishing attacks can be prevented with adequate staff security training.[14]

H. Plaintiff and Class Members Suffered Damages

58. The ramifications of Defendants' failure to keep employees' PII secure are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years. Consumer victims of data breaches are more likely to become victims of identity fraud.

59. The PII belonging to Plaintiff and Class Members is private, sensitive in nature, and was left inadequately protected by Defendants who did not obtain Plaintiff's or Class Members' consent to disclose such PII to any other person as required by applicable law and industry standards.

[12] https://insights.datamark.net/addressing-bpo-information-security/
[13] https://www.scmagazine.com/home/security-news/phishing/canon-breach-exposes-personal-data-of-current-former-ge-employees-beneficiaries/.
[14] https://www.passportalmsp.com/blog/security-awareness-training-can-protect-against-phishing-attacks.

60. The Data Breach was a direct and proximate result of Defendants' failure to: (a) properly safeguard and protect Plaintiff's and Class Members' PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (b) establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' PII; and (c) protect against reasonably foreseeable threats to the security or integrity of such information.

61. Defendants are both multi-billion-dollar companies and have the resources necessary to prevent the Data Breach, but neglected to adequately invest in data security measures, despite their obligation to protect consumer data.

62. Had Defendants remedied the deficiencies in their data security systems and adopted security measures recommended by experts in the field, they would have prevented the intrusions into their systems and, ultimately, the theft of PII.

63. As a direct and proximate result of Defendants' wrongful actions and inactions, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives. The U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."[15]

[15] U.S. Department of Justice, Office of Justice Programs Bureau of Justice Statistics, *Victims of Identity Theft, 2012*, December 2013 available at https://www.bjs.gov/content/pub/pdf/vit12.pdf

64. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GOA Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[16]

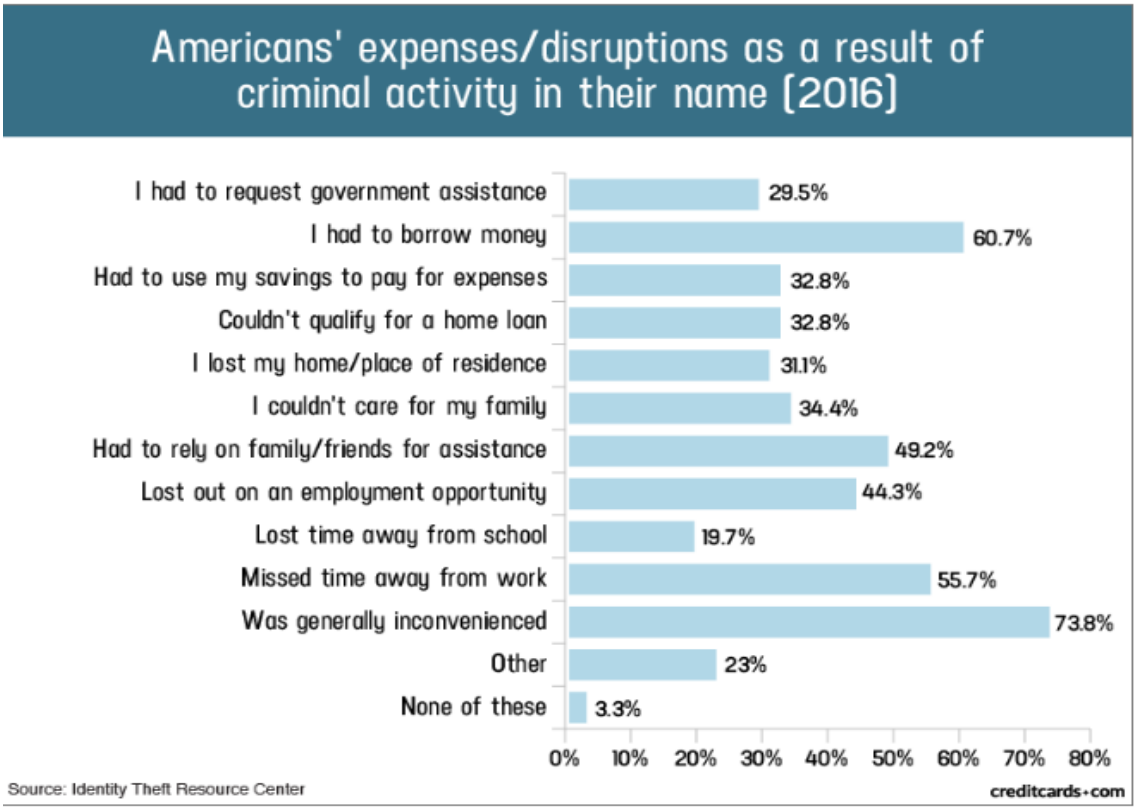
65. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[17]

66. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

67. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[18]

---

[16] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 12, 2019) ("GAO Report").
[17] *See* https://www.identitytheft.gov/Steps (last visited April 12, 2019).
[18] "Credit Card and ID Theft Statistics" by Jason Steele, 10/24/2017, at: https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited June 20, 2019).



68. What's more, PII constitutes a valuable property right, the theft of which is gravely serious.[19] Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

69. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs versus when it is discovered, and also between when PII and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may

[19] *See, e.g.*, John T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

> continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

70. PII and financial information are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

71. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future. Thus, Plaintiff and Class Members must vigilantly monitor their financial accounts for many years to come.

PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

72. To date, Defendants have merely offered identity theft and credit monitoring services at no charge for 24 months. The offer, however, is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and it entirely fails to provide any compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

73. Furthermore, Defendants' credit monitoring offer to Plaintiff and Class Members squarely places the burden on Plaintiff and Class Members, rather than on the Defendants, to investigate and protect themselves from Defendants' tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiff and Class Members in credit monitoring services upon discovery of the breach, Defendants merely sent instructions offering the services to affected employees, former employees, and their beneficiaries with the recommendation that they sign up for the services.

74. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

75. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

76. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

77. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

78. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

79. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

80. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

81. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

82. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

83. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

84. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendants, is protected from further breaches by

the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing personal and financial information is not accessible online and that access to such data is password-protected.

85. Further, as a result of Defendants' conduct, Plaintiff and Class Members are forced to live with the anxiety that their PII—which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

86. Plaintiff and the Class Members were also injured in that they were deprived of rights they possess under New York's General Business Law Section 349 to keep their PII secure and confidential.

87. As a direct and proximate result of Defendants' actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

88. What's more, Defendants' delay in identifying and reporting the Data Breach caused additional harm. It is axiomatic that "[t]he quicker a financial institution, credit card issuer, wireless carrier or other service provider is notified that fraud has occurred on an account, the sooner these organizations can act to limit the damage. Early notification can also help limit the liability of a victim in some cases, as well as allow more time for law enforcement to catch the fraudsters in the act."[20]

---

[20] *Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study*, Business Wire, https://www.businesswire.com/news/home/20170201005166/en/Identity-Fraud-Hits-Record-High-15.4-Million.

89. Indeed, once a data breach has occurred, "[o]ne thing that does matter is hearing about a data breach quickly. That alerts consumers to keep a tight watch on credit card bills and suspicious emails. It can prompt them to change passwords and freeze credit reports. And notifying officials can help them catch cybercriminals and warn other businesses of emerging dangers. If consumers don't know about a breach because it wasn't reported, they can't take action to protect themselves" (internal citations omitted).[21]

90. Although their PII was improperly exposed in February, affected consumers were not notified of the Data Breach until late-March, depriving them of the ability to promptly mitigate potential adverse consequences resulting from the Data Breach.

91. As a result of Defendants' delay in detecting and notifying consumers of the Data Breach, the risk of fraud for Plaintiff and Class Members has been driven even higher.

PARTIES

92. Plaintiff Steven Fowler is, and at all times mentioned herein was, an individual citizen of the State of Kentucky. Plaintiff Fowler is a former employee of GE. During Plaintiff Fowler's employment at GE, he was required to provide his PII to Defendant GE. On or about March 20, 2020, GE notified Plaintiff Fowler that his PII was stolen and compromised in the Data Breach.

93. Defendant Canon Business Process Services, Inc. is a Delaware corporation with its principal place of business at 261 Madison Ave., New York, New York, 10016.

---

[21]Consumer Reports, The Data Breach Next Door Security breaches don't just hit giants like Equifax and Marriott. Breaches at small companies put consumers at risk, too, January 31, 2019, https://www.consumerreports.org/data-theft/the-data-breach-next-door/

94. Defendant General Electric Company is a New York corporation with its principal place of business at 5 Necco Street, Boston, Massachusetts, 02210.

CLASS ACTION ALLEGATIONS

95. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class").

96. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> All persons whose PII was compromised as a result of the Data Breach announced by GE on or about March 20, 2020 (the "Class").

97. Excluded from the Class are Defendants' officers and directors, and any entity in which Defendants have a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendants. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

98. Plaintiff hereby reserves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

99. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, based on information and belief, the Class consists of hundreds of thousands of employees, former employees, and beneficiaries of Defendant GE whose data was compromised in the Data Breach.

100. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

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

f. Whether Defendant breached its duty to Class Members to safeguard their PII;

g. Whether computer hackers obtained Class Members' PII in the Data Breach;

h. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

i. Whether Plaintiff and Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

j. Whether Defendants' conduct was negligent;

k. Whether Defendants' conduct was *per se* negligent;

l. Whether Defendants' acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

m. Whether Defendants were unjustly enriched;

n. Whether Defendants violated the state consumer protection law asserted herein;

o. Whether Defendants failed to provide notice of the Data Breach in a timely manner; and

p. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

101. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class member, was compromised in the Data Breach.

102. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

103. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

104. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to

individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

105. Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

106. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the data breach.

107. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant GE.

CAUSES OF ACTION
FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

108. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 107 above as if fully set forth herein.

109. Defendant GE required Plaintiff and Class Members to submit non-public PII as a condition of employment or as a condition of receiving employee benefits.

110. Plaintiff and the Class Members entrusted their PII to Defendants with the understanding that Defendants would safeguard their information.

111. Defendants had full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

112. By assuming the responsibility to collect and store this data, and in fact doing so, and sharing it and using it for commercial gain, Defendants had a duty of care to use reasonable means to secure and safeguard their computer property—and Class Members' PII held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendants' duty included a responsibility to implement processes by which they could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

113. Defendants had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or

affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

114. Defendants' duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendants are bound by industry standards to protect confidential PII.

115. Defendants breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class Members' PII. The specific negligent acts and omissions committed by Defendants include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of their networks and systems;

c. Failing to periodically ensure that their email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' PII;

e. Failing to detect in a timely manner that Class Members' PII had been compromised; and

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

116. It was foreseeable that Defendants' failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the industry.

117. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

118. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect the PII and the harm suffered, or risk of imminent harm suffered by Plaintiff and the Class.

119. As a result of Defendants' negligence, Plaintiff and the Class Members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

120. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

121. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.,* (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

122. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 107 above as if fully set forth herein.

123. Plaintiff and Class Members were required to provide their PII to Defendants as a condition of their use of Defendants' services.

124. Plaintiff and Class Members paid money to Defendants in exchange for services, along with Defendants' promise to protect their PII from unauthorized disclosure.

125. In its written privacy policies, Defendant GE expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

126. Defendants further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

127. Implicit in the agreement between Plaintiff and Class Members and the Defendants to provide PII, was the latter's obligation to: (a) use such PII for business purposes only, (b) take reasonable steps to safeguard that PII, (c) prevent unauthorized disclosures of the PII, (d) provide Plaintiff and Class Members with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII, (e) reasonably safeguard and protect the PII of Plaintiff and Class Members from unauthorized disclosure or uses, and (f) retain the PII only under conditions that kept such information secure and confidential.

128. When Plaintiff and Class Members provided their PII to Defendant GE as a condition of their employment or employee beneficiary status, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

129. Defendants required Class Members to provide their PII as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their PII to Defendant.

130. In entering into such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendants' data security practices complied with relevant laws and regulations and were consistent with industry standards.

131. Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of the implied contract between them and Defendants to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

132. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendants.

133. Defendants breached their implied contracts with Class Members by failing to safeguard and protect their PII.

134. As a direct and proximate result of Defendants' breaches of the implied contracts, Class Members sustained damages as alleged herein.

135. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

136. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendants to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

137. Plaintiff restates and realleges paragraphs 1 through 107 above as if fully set forth herein.

138. Plaintiff and Class Members conferred a monetary benefit on Defendants. Specifically, Defendants enriched themselves by saving the costs they reasonably should have

expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendants' decision to prioritize their own profits over the requisite security.

139. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by industry standards.

140. Defendants acquired the PII through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

141. If Plaintiff and Class Members knew that Defendants had not secured their PII, they would not have agreed to provide their PII to Defendant GE.

142. Plaintiff and Class Members have no adequate remedy at law.

143. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PII, which

remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect PII in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

144. As a direct and proximate result of Defendants' conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

145. Defendants should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

FOURTH COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

146. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 107 above as if fully set forth herein.

147. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

148. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

149. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect employee PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

150. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendants' violation of the FTC Act establishes the duty and breach elements of negligence.

151. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

152. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

153. Pursuant to the Gramm-Leach-Bliley Act (15 U.S.C. § 6801), Defendants had a duty to protect the security and confidentiality of Plaintiff's and Class Members' PII.

154. Defendants breached their duties to Plaintiff and Class Members under the Gramm-Leach-Bliley Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' PII.

155. Defendants' failure to comply with applicable laws and regulations constitutes negligence *per se*.

156. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

157. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that they were failing to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

158. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FIFTH COUNT
VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT ("GBL")
(New York Gen. Bus. Law § 349)
(On Behalf of Plaintiff and All Class Members)

157. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 107 above as if fully set forth herein.

158. By the acts and conduct alleged herein, Defendants committed unfair or deceptive acts and practices by:

a) failing to maintain adequate computer systems and data security practices to safeguard PII;

b) failing to disclose that their computer systems and data security practices were inadequate to safeguard PII from theft;

c) continued gathering and storage of PII and other personal information after Defendants knew or should have known of the security vulnerabilities of their computer systems that were exploited in the Data Breach;

d) making and using false promises, set out in the Privacy Notice, about the privacy and security of PII of Plaintiff and Class Members, and;

e) continued gathering and storage of PII and other personal information after Defendants knew or should have known of the Data Breach and before Defendants allegedly remediated the data security incident.

159. These unfair acts and practices violated duties imposed by laws, including but not limited to the Federal Trade Commission Act, HIPAA, the Gramm- Leach-Bliley Act, and NY GBL § 349.

160. The foregoing deceptive acts and practices were directed at consumers.

161. The foregoing deceptive acts and practices are misleading in a material way because they fundamentally misrepresent the character of the services provided, specifically as to the safety and security of PII.

162. Defendants' unconscionable commercial practices, false promises, misrepresentations, and omissions set forth in this Complaint are material in that they relate to matters which reasonable persons, including Plaintiff and members of the Class, would attach importance to in making their decisions and/or conducting themselves regarding the services received from Defendants.

163. Plaintiff and Class members are consumers who made payments to Defendants for the furnishing of employment benefit services that were primarily for personal, family, or household purposes.

164. Defendants engaged in the conduct alleged in this Complaint, entering into transactions intended to result, and which did result, in the furnishing of employment benefit services to consumers, including Plaintiff and Class Members.

165. Defendants engaged in, and its acts and omissions affect, trade and commerce, or the furnishing of services in the State of New York.

166. Defendants' acts, practices, and omissions were done in the course of Defendants' business of furnishing employment benefit services to consumers in the State of New York.

167. As a direct and proximate result of Defendant's multiple, separate violations of GBL §349, Plaintiff and the Class Members suffered damages including, but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

168. Also as a direct result of Defendants' violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

169. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect

Plaintiff, Class Members and the public from Defendants' unfair, deceptive, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

170. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' PII and that the risk of a data security incident was high.

171. Plaintiff and Class Members were injured because: a) they would not have paid for employment benefit services from Defendants had they known the true nature and character of Defendants' data security practices; b) Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of promises that Defendants would keep their information reasonably secure, and c) Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

172. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

173. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

SIXTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

174. Plaintiff re-alleges and incorporates by reference Paragraphs 1 through 107 above as if fully set forth herein.

175. In light of the special relationship between Defendant GE and Plaintiff and Class Members, whereby Defendants became guardians of Plaintiff's and Class Members' PII,

Defendants became fiduciaries by their undertaking and guardianship of the PII, to act primarily for the benefit of GE's employee, former employees, and their beneficiaries, including Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' PII; (2) to timely notify Plaintiff and Class Members of a data breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendants did and does store.

176. As the agent of Defendant GE for purposes of storing, maintaining, and safeguarding Plaintiff's and Class Members' PII, Defendant GE's fiduciary duty is imputed to Defendant Canon.

177. Defendants have a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of GE's relationship with its employees, former employees and beneficiaries, in particular, to keep secure their PII.

178. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to diligently discovery, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

179. Defendants breached their fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' PII.

180. Defendants breached their fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

181. Defendants breached their fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' PII.

182. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i)

actual identity theft; (ii) the compromise, publication, and/or theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in their continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendants' services they received.

183. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a class action and appointing Plaintiff and his counsel to represent the Class;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c) For equitable relief compelling Defendants to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

e) Ordering Defendants to pay for not less than seven years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: April 8, 2020

Respectfully submitted,

BURSOR & FISHER, P.A.

/s/ Philip L. Fraietta

Philip L. Fraietta
Alec M. Leslie
888 7th Avenue
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163

Email: pfraietta@bursor.com
aleslie@bursor.com

BURSOR & FISHER, P.A.
L. Timothy Fisher*
1990 North California Blvd., Suite 940
Walnut Creek, CA. 94596
Tel: (925) 300-4455
Fax: (925) 407-2700
Email: ltfisher@bursor.com

Gary E. Mason*
David K. Lietz*
MASON LIETZ & KLINGER LLP
5301 Wisconsin Avenue, NW
Suite 305
Washington, DC 20016
Tel: (202) 429-2290
gmason@masonllp.com
dlietz@masonllp.com

Gary M. Klinger*
MASON LIETZ & KLINGER LLP
227 W. Monroe Street, Suite 2100
Chicago, IL 60630
Tel.: (312) 283-3814
gklinger@masonllp.com

**pro hac vice to be filed*

Attorneys for Plaintiff

ClassAction.org