UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

IN RE: GE/CBPS DATA BREACH LITIGATION	Civil Action No.: 1:20-cv-02903-KPF **CONSOLIDATED CLASS ACTION COMPLAINT**

Plaintiffs Steven Fowler and Maher Baz ("Plaintiffs"), individually and on behalf of all others similarly situated (the "Class" or "Class members"), bring this Class Action Complaint against Defendants General Electric Company and Canon Business Process Services, Inc., based on their individual experiences and personal information, and the investigation of their counsel.

INTRODUCTION

1. Plaintiffs Steven Fowler and Maher Baz, individually and on behalf of all others similarly situated, bring this class action suit against Defendants because of Defendants' failure to safeguard the confidential information of thousands of current and former General Electric Company employees and their beneficiaries. The confidential information stolen includes financial information (*e.g.,* bank account information, such as bank routing numbers and checking account numbers) and personal information (*e.g.,* Social Security Numbers, passport numbers, and driver's license numbers) (collectively, " Personal Financial Information" or "PFI").

2. General Electric Company ("GE") is one of the largest companies in the United States, both in terms of gross revenue and number of employees. An employer of over 200,000 people worldwide, GE collects significant data on its current and former employees, and their beneficiaries. This data often includes sensitive personal information obtained in the context of an

employment relationship, such as Social Security numbers, addresses, driver's license numbers, bank information, passport numbers, dates of birth, and medical child support orders.

3. GE in turn provides some of this personal and financial information to its vendors. Specifically, GE contracts with Defendant Canon Business Process Services, Inc. ("Canon"), one of its vendors, to process current and former GE employees' documents and beneficiary-related documents of GE's employees.

4. On March 20, 2020, GE announced that an unauthorized person accessed a Canon email account that contained documents with Personal Financial Information of current and former GE employees and beneficiaries of GE's employees (the "Data Breach"). The information accessed included, but was not limited to, Plaintiffs' and Class members' names, addresses, dates of birth, Social Security numbers, driver's license numbers, passport numbers, financial information, such as bank account numbers, and beneficiary designation information. GE further revealed that the exposure occurred between February 3, 2020 and February 14, 2020.

5. The confidential information that was compromised in the Data Breach is considered a treasure trove that can be sold on the Dark Web and to other criminals, or to carry out identity theft or other fraud. Industry security reports indicate that the Data Breach was likely the result of an elementary attack, such as phishing or using keyboard-logging malware to steal password information. One thing is clear: the Data Breach could have been avoided through basic security measures, including multifactor authentication and user security training.

6. At all relevant times, GE promised and agreed in various documents to safeguard and protect Personal Financial Information in accordance with federal, state, and local laws, and industry standards. GE made these promises and agreements in its employee handbook, titled "THE SPIRIT & THE LETTER," its Employment Data Protection Standards, its Commitment to

the Protection of Personal Information, and other written notices and also extended this commitment to situations in which third parties, such as Canon, handled PFI on GE's behalf.

7. Contrary to these promises, and despite the fact that the threat of a data breach has been a well-known risk to Defendants, especially due to the valuable and sensitive nature of the data Defendants collect, store and maintain, Defendants failed to take reasonable steps to adequately protect the PFI of current and former GE employees and their beneficiaries. The data breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect PFI.

8. As a result of Defendants' failure to take reasonable steps to adequately protect the ultra-sensitive PFI of current and former GE employees and their beneficiaries, Plaintiffs' and Class members' PFI is now in the hands of thieves which can now be sold on the Dark Web and to commit identity theft and fraud for the foreseeable future.

9. Defendants' failure to implement and follow basic security procedures has resulted in ongoing harm to Plaintiffs and Class members who will continue to experience a lack of data security for the indefinite future and remain at serious risk of identity theft and fraud that would result in significant monetary loss.

10. Accordingly, Plaintiffs seek to recover damages and other relief resulting from the Data Breach, including but not limited to, compensatory damages, reimbursement of costs that Plaintiffs and others similarly situated will be forced to bear, and declaratory judgment and injunctive relief to mitigate future harms that are certain to occur in light of the scope of this breach.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5 million,

exclusive of interest and costs; the number of members of each of the proposed Class exceeds 100; and minimal diversity exists because at least one Plaintiffs and Defendants are citizens of different states. This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

12. This Court has personal jurisdiction over Defendant GE as it is incorporated in this State. Additionally, GE conducts substantial business in this State and in this District and/or the conduct complained of occurred in and/or emanated from this State and District because the confidential information compromised in Data Breach was likely stored and/or maintained in accordance with practices emanating from this District.

13. This Court also has personal jurisdiction over Defendant Canon, as Canon's principal place of business is in this State and District. Additionally, Canon conducts substantial business in this State and in this District and/or the conduct complained of occurred in and/or emanated from this State and District because the confidential information compromised in Data Breach was likely stored and/or maintained in accordance with practices emanating in this District.

14. Venue is proper pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and/or emanated from this District. Venue is additionally proper because Defendant Canon, GE's service provider for handling PFI on GE's behalf, has its principal place of business in this District.

THE PARTIES

A. Plaintiff Maher Baz

15. Plaintiff Maher Baz is a citizen and resident of the State of Florida, residing in Orlando.

16. Plaintiff Baz was employed by GE from 1998 to 2010 and from 2016 to July 11, 2019. As a condition of employment, Plaintiff Baz was required to provide GE with his personal and financial information, including his Social Security Number, bank and financial account information, such as routing and checking account numbers, tax information, date of birth, and his name and address. Plaintiff Baz also provided GE with personal information relating to his beneficiaries, including his daughter. GE collected, stored, and used Plaintiff Baz' Personal Financial Information for employment purposes.

17. Sometime after February 14, 2020, Plaintiff Baz experienced identity theft. On or around April 2020, Plaintiff Baz discovered, through his online banking statement, fraudulent charges to his bank account. Apart from the Data Breach, Plaintiff Baz is unaware of any other breaches where his PFI was compromised within the last year and he has not received any notifications of other data breaches in the last year notifying him that his PFI has been compromised.

18. In or around February 2020 and March 2020, Plaintiff Baz has also received electronic solicitations to his LinkedIn account regarding his Social Security Number and his date of birth that have caused him to waste countless hours mitigating the damage from this breach.

19. On May 2, 2020, Mr. Baz learned that his 2019 electronic federal tax return filing was rejected because his daughter's Social Security number was fraudulently used by an unauthorized person. Mr. Baz had provided his daughter's information, including her Social Security number, to GE for beneficiary designation purposes. Apart from the Data Breach, his daughter is unaware of any other data breaches where her PFI was compromised within the last year and she has not received any notifications of other data breaches in the last year notifying her that her PFI has been compromised.

20. As a result of the Data Breach, Plaintiff Baz had to schedule an appointment to go to the bank, as banking services are available by appointment only due to the COVID-19 crisis. He spent time and money driving to and from the bank to resolve the fraudulent activity. He also spent time making multiple telephone calls to the IRS to resolve the rejection of his 2019 electronic federal tax return filing. As a result of the unauthorized use of his daugher's Social Security number, Mr. Baz's tax refund was delayed. Plaintiff Baz continues to spend time and effort researching and monitoring his financial accounts and social media accounts in an effort to detect and prevent any further misuse and unauthorized access.

B. Plaintiff Steven Fowler

21. 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 PFI to Defendant GE. On or about March 20, 2020, GE notified Plaintiff Fowler that his PFI was stolen and compromised in the Data Breach.

C. Defendant General Electric Company

22. Defendant General Electric Company is a New York corporation and is headquartered in Boston, Massachusetts.

D. Defendant Canon Business Process Services, Inc.

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

FACTUAL ALLEGATIONS

A. General Electric Company.

24. GE is a high-tech industrial company that operates worldwide through four industrial segments: power; renewable energy; aviation; and healthcare. GE claims, "For more

than 125 years, GE has invented the future of industry. Our vast and valuable installed base across aviation, power, healthcare and renewable energy keeps us intimately involved in the daily operations of our customers around the world."[1]

25. GE employs a large number of individuals, both internationally and in the United States. At year-end 2019, GE employed approximately 205,000 people, with approximately 70,000 employed in the United States.

26. To attract talent and remain competitive in the various industries in which it operates, GE touts both its compensation and benefits, including benefits for former employees. GE's website states, "At GE, we recognize how important a well-rounded career is to you and your family. To ensure you get the most out of your employment, we offer a full suite of tools that cover everything from your career to your compensation and benefits."[2] GE notes that it provides employees: disability coverage; medical, dental, and vision plans; and retirement savings and matching, among other benefits.

27. As a condition of employment, GE collects and maintains personal and financial information about its employees. According to GE, "personal information" is "employment data obtained in the context of an employment relationship" and "any information relating to a directly or indirectly identifiable person []; examples include name, address, email, phone, national identifier and credit card number."[3] Further, GE defines "employment data" as "any information about an identified or identifiable person that is obtained in the context of a person's working

[1] ABOUT GE, https://www.ge.com/about-us (last visited Apr. 16, 2020).
[2] GE CAREER BENEFITS, https://jobs.gecareers.com/global/en/ge-career-benefits (last visited Apr. 16, 2020).
[3] *See* https://www.ge.com/bcr (last visited Apr. 17, 2020) and GE's employee handbook, THE SPIRIT & THE LETTER, https://www.ge.com/in/sites/www.ge.com.in/files/TheSpirit&TheLetter.pdf (last visited Apr. 17, 2020).

relationship with a GE entity. Such persons include, for example, 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."[4]

28. GE also offers certain benefits to its former employees, and its website offers these individuals access to GE pay, benefit, and human resource services.

29. GE contracts with Defendant Canon to process current and former GE employees' documents and beneficiary-related documents of GE's employees.

B. GE Promised to Protect the Personal Financial Information of Its Current and Former Employees and Beneficiaries of GE's Employees.

30. GE emphasizes its purported commitment to its protection of Personal Financial Information. GE's website claims:

> GE respects the privacy rights of individuals and is committed to handling Personal Information responsibly, in accordance with applicable law, applicable contractual obligations, and GE's Commitment to the Protection of Personal Information (the Commitment), described below. The Commitment sets out GE's principles for the processing of Personal Information by and on behalf of GE.
>
> The Commitment establishes a legal basis for cross-border transfers of Personal Information within the GE Group (all wholly or majority-owned divisions of GE Company, including Electric Insurance Company and its subsidiaries), including where GE Group members adhere to relevant parts of the Commitment as data processors. Additionally, GE may carry out cross-border transfers of Personal Information to third parties outside the GE Group in accordance with applicable law. GE will handle Personal Information in accordance with the Commitment where applicable, unless in conflict with stricter requirements of local law, in which case local law will prevail. . . .
>
> The Commitment is designed to ensure that Personal Information will be protected regardless of geography or technology, when used

[4] https://www.ge.com/content/dam/gepower-pw/global/en_US/documents/ec-supplier/ _ Employee _ Data _ Protection_Standards.pdf (last visited Apr. 17, 2020).

> within the GE Group, and applies to GE's processing of GE Personal Information and GE Customer Personal Information.[5]

31. GE's "commitment" continues, describing particular promises to protect the sensitive PFI that it gathers:

> GE strives to protect Personal Information with appropriate technical and organizational measures to ensure its integrity, confidentiality, security and availability. GE will inform individuals of a security breach affecting their GE Personal Information that could pose a high risk to their individual rights and freedoms. In accordance with applicable law, GE will provide reasonable assistance to Customers, where GE is a processor, to ensure the security of their processing and will inform GE Customers of a security breach of GE Customer Personal Information as required under such laws.[6]

32. For the preceding "commitment," GE defines "personal information" as "any information relating to an identified or identifiable person."

33. According to GE's employee handbook, THE SPIRIT & THE LETTER, "GE respects individual privacy rights. GE is committed to collecting, handling and protecting Personal Information responsibly, and in compliance with applicable privacy and information security laws and with GE's Commitment to the Protection of Personal Information (GE's Binding Corporate Rules), where applicable."[7]

34. Moreover, GE's further commitment is evidenced by its establishment of the Employment Data Protection Standards, which details and outlines the information it collects from

---

[5] GE'S COMMITMENT TO THE PROTECTION OF PERSONAL INFORMATION, https://www.ge.com/bcr (last visited Apr. 16, 2020).
[6] *Id.*
[7] THE SPIRIT & THE LETTER, https://www.ge.com/in/sites/www.ge.com.in/files/TheSpirit&TheLetter.pdf (last visited Apr. 17, 2020).

employees and its standards to secure and protect employment data.[8] "The aim of these Employment Data Protection Standards ("Standards") is to provide adequate and consistent safeguards for the handling of employment data by GE entities."

35. In its Standards, GE represents to its employees that "GE respects the privacy rights and interests of each individual. 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."[9]

[8] https://www.ge.com/content/dam/gepower-pw/global/en_US/documents/ec-supplier/ GE_ Employee_ Data_Protection_Standards.pdf (last visited Apr. 17, 2020).
[9] *Id.*

36. GE further represents in its Standards 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."[10]

37. Accordingly, GE outlines in its Standards the following measures it takes to protect PFI:

> **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.

[10] *Id.*

38. Based on these representations, GE's current and former employees reasonably believed that GE, and any third parties GE contracted with, would protect their Personal Financial Information, including the PFI of their beneficiaries.

39. Furthermore, as part of GE's employment guidelines, GE instructs its employees to do the following:

- "Limit access to GE information to authorized individuals who need it for legitimate business purposes.
- Prevent unauthorized access, accidental loss, disclosure or destruction of GE information:
    - Secure physical copies and storage areas.
    - Use strong passwords; don't share your password with anyone.
    - Use only GE-approved systems and tools for storage, transmission and backup of GE information. Do not use personal email, unapproved devices or software to conduct GE business.
    - When posting information online, do not disclose Personal Information, trade secrets, proprietary or other commercially sensitive information.
    - Know the signs of phishing and recognize efforts to improperly acquire GE information.
- Consult with your privacy leader before implementing new or significantly modified processes that use Personal Information, including new software or code."[11]

[11] THE SPIRIT & THE LETTER, https://www.ge.com/in/sites/www.ge.com.in/files/TheSpirit&TheLetter.pdf (last visited Apr. 17, 2020).

40. Yet, GE itself has failed on all counts when it comes to security. GE failed to maintain the confidentiality of PFI, failed to prevent cybercriminals from access and use of PFI, failed to avoid accidental loss, disclosure, or unauthorized access to PFI, failed to prevent the unauthorized disclosure of PFI outside of GE, and failed to provide security measures consistent with industry standards for the protection of PFI, of its current and former employees and the beneficiaries of GE's employees.

C. The Data Breach.

41. To assist with GE's business administration, GE provides Personal Financial Information to Canon, one of GE's vendors. Specifically, GE contracts with Canon to process current and former GE employees' documents and beneficiary-related documents of GE's employees.

42. Canon Business Process Services is a "leading provider of business process services, document management and managed workforce services, dedicated to helping our clients build stronger and more agile businesses . . . We foster growth and manage operations through a range of services encompassing information and document management, business process, outsourcing, managed workforce services, source-to-pay outsourcing services, insurance processing, logistics management, records management and information governance, legal discovery services, print services, and financial services application processing."[12]

43. On March 20, 2020, GE revealed in a notice of data breach filed with various governmental agencies, that Canon had one of its employee email accounts breached by an unauthorized party in February 2020.

44. The notice states:

[12] CANON BUSINESS PROCESS OUTSOURCING, https://cbps.canon.com (last visited Apr. 16, 2020).

> 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. . . .
>
> 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.

45. Despite being notified on February 28, 2020 of the Data Breach, GE waited almost a month before disclosing the breach to the public.

46. According to Roger Grimes, a cyber-security expert and a 30-year computer security consultant, the Data Breach appears to have been caused by "using a standard credential phishing attack or due to credential reuse on another site."[13]

47. Cyber-security experts have stated that phishing attacks can be prevented with robust staff security awareness training.[14]

48. Accordingly, unauthorized parties accessed and/or removed documents containing personal and financial information on GE's current and former employees and their beneficiaries,

---

[13] https://www.scmagazine.com/home/security-news/phishing/canon-breach-exposes-personal-data-of-current-former-ge-employees-beneficiaries/ (last visited Apr. 18, 2020).

[14] *See* https://securityintelligence.com/articles/how-to-protect-your-organization-from-evolving-phishing-attacks/ (last visited Apr. 18, 2020). *See also* https://www.passportalmsp.com/blog/security-awareness-training-can-protect-against-phishing-attacks (last visited Apr. 18, 2020).

including, but not limited to, their names, addresses, Social Security numbers, driver's license numbers, bank account numbers, passport numbers, dates of birth, and other private and confidential information, from its vendor, Canon's email account.

D. The Data Breach was a Foreseeable Risk of which Defendants were on Notice.

49. In the last several years, there has been a wave of data breaches. The threat of hackers gaining access to information that businesses store is serious and well-known. Government authorities have been advising that companies take precautions to prevent these hacks for years.

50. Since at least 2015, the Federal Bureau of Investigation ("FBI") has specifically advised private industry about the threat of "Business E-Mail Compromise" ("BEC"). The FBI calls BEC "a growing financial fraud that is more sophisticated than any similar scam the FBI has seen before and one—in its various forms—that has resulted in actual and attempted losses of more than a billion dollars to businesses worldwide." The FBI notes that "scammers' methods are extremely sophisticated," and warns companies that "the criminals often employ malware to infiltrate company networks . . . ."[15]

51. In both 2016 and 2017, the IRS warned that criminals were using spoofing emails from executives in the company.[16] These emails will look legitimate, like they came from the CEO or CFO of the recipient's company, and will request a list of employees and information, such as social security numbers.

---

[15] BUSINESS E-MAIL COMPROMISE: AN EMERGING GLOBAL THREAT, https://www.fbi.gov/news/stories/business-e-mail-compromise (last visited Apr. 16, 2020).

[16] "IRS Alerts Payroll and HR Professionals to Phishing Scheme Involving W-2s," IRS Press Release No. IR-2016-34 (March 1, 2016), https://www.irs.gov/newsroom/irs-alerts-payroll-and-hr-professionals-to-phishing-scheme-involving-w-2s (last visited Apr. 20, 2020); "Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others," Internal Revenue Service Press Release No. IR-2017-20 (Feb. 2, 2017), https://www.irs.gov/newsroom/dangerous-w-2-phishing-scam-evolving-targeting-schools-restaurants-hospitals-tribal-groups-and-others (last visited Apr. 20, 2020).

52. These emails are designed to trick companies into thinking they are legitimate requests by company executives and into sending the requested information. The scammer can then use the information for a wide variety of identity fraud, including filing fraudulent tax returns; opening credit card and bank accounts; obtaining loans; opening utility accounts; and filing for student aid, among other things.

53. GE contemplated providing PFI to third party vendors and provided assurances that GE would protect PFI. As noted *supra* in GE's commitment to protect PFI, GE's website states, "GE may carry out cross-border transfers of Personal Information to third parties outside the GE Group in accordance with applicable law. GE will handle Personal Information in accordance with the Commitment where applicable, unless in conflict with stricter requirements of local law, in which case local law will prevail."[17]

54. Indeed, GE's filings with the Securities and Exchange Commission ("SEC") show the extent to which GE foresaw such an attack. In the Form 10-K that GE filed with the SEC on February 26, 2019, GE identified "cybersecurity" as a risk factor facing the company, even acknowledging that a third party might be the target of a hacker. GE specifically stated:

> Increased global cybersecurity vulnerabilities, threats, computer viruses and more sophisticated and targeted cyber-related attacks, as well as cybersecurity failures resulting from human error and technological errors, pose a risk to the security of GE's and its customers', partners', suppliers' and third-party service providers' products, systems and networks and the confidentiality, availability and integrity of GE's and its customers' data. As the perpetrators of such attacks become more capable, and as critical infrastructure is increasingly becoming digitized, the risks in this area continue to grow. . . .[18]

[17] GE'S COMMITMENT TO THE PROTECTION OF PERSONAL INFORMATION, https://www.ge.com/bcr (last visited Apr. 16, 2020).
[18] General Electric Co., Annual Report (Form 10-K) (Feb. 26, 2019), at 82.

55. Accordingly, both GE and Canon knew, given the vast amount of PFI it collects, manages, and maintains, that they were a target of security threats, and therefore understood the risks posed by unsecure data security practices and systems. Defendants' failure to heed warnings and to otherwise maintain adequate security practices resulted in this Data Breach.

E. Defendants, At All Relevant Times, Had A Duty to Plaintiffs and Class Members to Properly Secure their PFI.

56. Defendants, at all relevant times, had a duty to Plaintiffs and Class members to properly secure their PFI, encrypt and maintain such information using industry standard methods, train their employees, utilize available technology to defend their systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class members, and promptly notify Plaintiffs and Class members when Defendants became aware of the potential that its current and former employees' PFI, and the beneficiaries' PFI of GE's employees may have been compromised.

57. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants, on the one hand, and Plaintiffs and the Class members, on the other hand. The special relationship arose because Plaintiffs and the members of the Class entrusted GE with their PFI as part of receiving compensation and/or benefits from GE, and GE entrusted the PFI to Cannon. Defendants had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite their obligation to protect such information. Accordingly, Defendants breached their common law, statutory, and other duties owed to Plaintiffs and Class members.

58. Defendants' duty to use reasonable security measures also arose 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 sue reasonable measures to protect confidential data by entities like Defendant.

59. The Data Breach was a direct and proximate result of Defendants' failure to: (1) properly safeguard and protect Plaintiffs' and Class members' PFI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and common law; (2) establish and implement appropriate safeguards to ensure the security and confidentiality of Plaintiffs' and Class members' PFI; and (3) protect against reasonably foreseeable threats to the security or integrity of such information.

F. Defendants Failed to Comply with Industry Standards to Protect Against the Data Breach.

60. The Federal Trade Commission has established data security principles and practices for businesses as set forth in its publication, *Protecting Personal Information: A Guide for Business*.[19] Among other things, the FTC states that companies should encrypt information stored on computer networks and dispose of consumer information that is no longer needed. The FTC also says to implement policies for installing vendor-approved patches to correct problems, and to identify operating systems. The FTC also recommends that companies understand their network's vulnerabilities and develop and implement policies to rectify security deficiencies. Further, the FTC recommends that companies utilize an intrusion detection system to expose a data breach as soon as it occurs; monitor all incoming traffic for activity that might indicate unauthorized access into the system; monitor large amounts of data transmitted from the system; and have a response plan ready in the event of a data breach.

[19] https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Apr. 18, 2020).

61. In another FTC publication, *Start with Security: A Guide for Business*, the FTC recommends, among other things, that companies "make sure [third-party] service providers implement reasonable security measures."[20]

62. The FTC has prosecuted a number of enforcement actions against companies for failing to take measures to adequately and reasonably protect consumer data. The FTC has viewed and treated such security lapses as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.

63. Defendants failed to maintain reasonable data security procedures and practices. GE also failed to implement reasonable security procedures and practices to prevent cyber attackers from unauthorized access to its services provider's computer systems. Defendants' failure to maintain and implement reasonable and appropriate measures to protect against unauthorized access to consumer PFI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

64. Accordingly, Defendants did not comply with legal state and federal law requirements and industry standards, as discussed *supra*.

65. Defendants were at all times fully aware of their obligations to protect the PFI of current and former employees and of the beneficiaries of GE's employees. Defendants were also aware of the significant consequences that would result from its failure to do so.

G. <u>Plaintiffs and Class Members Have Been Injured and Will Suffer Additional Harm.</u>

66. 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

[20] https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Apr. 18, 2020).

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 Plaintiffs' and Class Members' PII.

67. Furthermore, Defendants' credit monitoring offer to Plaintiffs and Class Members squarely places the burden on Plaintiffs and Class Members, rather than on the Defendant, to investigate and protect themselves from Defendants' tortious acts resulting in the Data Breach. Rather than automatically enrolling Plaintiffs 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.

68. As a result of the data breach and Defendants' failure to provide timely notice to Plaintiff and Class members, Plaintiffs' and Class members' PFI, including information associated with their beneficiaries, are now in the hands of unknown hackers, and Plaintiffs and Class members now face an imminent heightened, and substantial risk of identity theft and other fraud, which is a concrete and particularized injury traceable to Defendants' conduct. Accordingly, Plaintiff and the Classes have suffered "injury-in-fact." *See Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).

69. The consequences of Defendants' failure to keep Plaintiffs' and Class members' PFI and all information associated with their PFI secure and protected are severe.

70. Thieves are already using the PFI stolen to commit actual fraud, as occurred to Plaintiffs as alleged herein.

71. Theft of personal and financial information is a serious and growing problem in the United States. Personal and financial information is a valuable commodity to identity thieves. As

cyber security journalists have recognized, the PFI 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."[21]

72. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[22] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[23]

73. The United States Government Accountability Office noted in a June 2007 report on Data Breaches ("GAO Report") that identify thieves use identifying data such as Social Security Numbers to open financial accounts, receive government benefits and incur charges and credit in a person's name.[24] As the GAO Report states, this type of identity theft is the most harmful because it often takes some time for the victim to become aware of the theft, and the theft can impact the victim's credit rating adversely.

---

[21] https://www.tripwire.com/state-of-security/featured/ge-data-breach-third-party/ (last visited Apr. 18, 2020); *see also* https://threatpost.com/ge-employees-sensitive-hr-doc-breach/154136/ (last visited Apr. 18, 2020) and https://www.cpomagazine.com/cyber-security/third-party-data-breach-of-ge-vendor-exposes-highly-sensitive-employee-information/ (last visited Apr. 18, 2020).

[22] 17 C.F.R. § 248.201 (2013).

[23] *Id.*

[24] *See Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent Is Unknown* (June 2007), United States Government Accountability Office, *available at* https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 16, 2020), at 9.

74. Accordingly, identify theft victims must spend countless hours and large amounts of money repairing the impact to their credit.[25]

75. PFI is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years. According to the GAO Report:

> [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 continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[26]

76. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[27]

77. Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

---

[25] *Guide for Assisting Identity Theft Victims*, Federal Trade Commission, 4 (September 2013), *available at* http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf (last visited Apr. 16, 2020).

[26] United States Government Accountability Office, *supra* note 11, at 29.

[27] Elinor Mills, *Study: Medical identity theft is costly for victims,* CNET (Mar. 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited Apr. 16, 2020).

78. For all the above reasons, Plaintiffs and Class members have suffered harm; and there is a substantial risk of injury to Plaintiffs and Class members that is imminent and concrete and that will continue for years to come.

79. As a direct and proximate result of Defendants' wrongful actions and inaction, Plaintiffs and Class members have suffered injury and damages, including the increased risk of identity theft and identity fraud, improper disclosure of PFI, the time and expense necessary to mitigate, remediate, and sort out the increased risk of identity theft and the inability to use debit cards because those cards were canceled, suspended, or otherwise rendered unusable as a result of the data breach, and/or false or fraudulent charges stemming from the data breaches.

CLASS ACTION ALLEGATIONS

80. Plaintiffs bring this action and seek to certify and maintain it as a class action under Federal Rules of Civil Procedure 23(a), (b)(2), (b)(3), and/or (c)(4), on behalf of himself, and the following proposed Classes (collectively, the "Class"):

81. The **Nationwide Class** is defined as follows: All individuals residing in the United States whose Personal Financial Information was compromised in the data breach initially disclosed by GE in or about March 2020.

82. The **Florida Class** is defined as follows: All individuals residing in Florida whose Personal Financial Information was compromised in the data breach initially disclosed by GE in or about March 2020.

83. The **GE Employee Class** is defined as follows: All current and former employees of GE whose Personal Financial Information was compromised in the data breach initially disclosed by GE in or about March 2020.

84. Excluded from each of the above proposed Classes are: Defendants, any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns of Defendants; and judicial officers to whom this case is assigned and their immediate family members.

85. Plaintiffs reserve the right to re-define the Class definitions after conducting discovery.

86. Each of the proposed Classes meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and/or (c)(4).

87. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Pursuant to Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, the proposed Class includes potentially tens of thousands of individuals whose Personal Financial Information was compromised in the Data Breach. Class members may be identified through objective means, including by and through Defendants' business records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

88. **Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3).** Pursuant to Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

(a) Whether Defendants had a legal duty to implement and maintain reasonable security procedures and practices for the protection of Class members' personal and financial information, including by vendors;

(b) Whether Defendants breached their legal duty to implement and maintain reasonable security procedures and practices for the protection of Plaintiffs and Class members' personal and financial information;

(c) Whether Defendants' conduct, practices, actions, and omissions, resulted in or were the proximate cause of the data breach, resulting in the loss of personal and financial information of Plaintiffs and Class members;

(d) Whether Defendants had a legal duty to provide timely and accurate notice of the data breach to Plaintiffs and Class members;

(e) Whether Defendants breached their duty to provide timely and accurate notice of the data breach to Plaintiffs and Class members;

(f) Whether and when Defendants knew or should have known that Canon's computer systems were vulnerable to attack;

(g) Whether Defendants failed to implement and maintain reasonable and adequate security measures, procedures, and practices to safeguard Plaintiffs' and Class members' personal and financial information, including by vendors;

(h) Whether Defendants breached express or implied contracts with Plaintiffs and the Class in failing to have adequate data security measures despite promising to do so;

(i) Whether Defendants' conduct was negligent;

(j) Whether Defendants' conduct was *per se* negligent;

(k) Whether Defendants' practices, actions, and omissions constitute unfair or deceptive business practices;

(l) Whether Plaintiffs and Class members suffered legally cognizable damages as a result of Defendants' conduct, including increased risk of identity theft and loss of value of their personal and financial information; and

(m) Whether Plaintiffs and Class members are entitled to relief, including damages and equitable relief.

89. **Typicality. Fed. R. Civ. P. 23(a)(3).** Pursuant to Rule 23(a)(3), Plaintiffs' claims are typical of the claims of the members of the Class. Plaintiffs, like all members of the Class, was injured through Defendants' uniform misconduct described above and asserts similar claims for relief. The same events and conduct that give rise to Plaintiffs' claims also give rise to the claims of every other Class member because Plaintiffs and each Class member is a person that has suffered harm as a direct result of the same conduct engaged in by Defendants and resulting in the data breach.

90. **Adequacy of Representation (Fed. R. Civ. P. 23(a)(4)**. Pursuant to Rule 23(a)(4), Plaintiffs and their counsel will fairly and adequately represent the interests of the Class members. Plaintiffs have no interest antagonistic to, or in conflict with, the interests of the Class members. Plaintiffs' lawyers are highly experienced in the prosecution of consumer class actions and data breach cases.

91. **Superiority (Fed. R. Civ. P. 23(b)(3)**. Pursuant to Rule 23(b)(3), a class action is superior to individual adjudications of this controversy. Litigation is not economically feasible for individual members of the Class because the amount of monetary relief available to individual plaintiffs is insufficient in the absence of the class action procedure. Separate litigation could yield

inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. A class action presents fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

92. **Risk of Inconsistent or Dispositive Adjudications and the Appropriateness of Final Injunctive or Declaratory Relief (Fed. R. Civ. P. 23(b)(1) and (2)).** In the alternative, this action may properly be maintained as a class action, because:

(a) the prosecution of separate actions by individual members of the Class would create a risk of inconsistent or varying adjudication with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendants; or

(b) the prosecution of separate actions by individual members of the Class would create a risk of adjudications with respect to individual members of the Class which would, as a practical matter, be dispositive of the interests of other members of the Class not parties to the adjudications, or substantially impair or impede their ability to protect their interests; or

(c) Defendants have acted or refused to act on grounds generally applicable to the Class, thereby making appropriate final injunctive or corresponding declaratory relief with respect to the Class as a whole.

93. **Issue Certification (Fed. R. Civ. P. 23(c)(4)**. In the alternative, the common questions of fact and law, set forth in Paragraph 87, are appropriate for issue certification on behalf of the proposed Class.

COUNT I

NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class, Or, Alternatively, Plaintiff Baz and the Florida Class)

94. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

95. GE required Plaintiffs and Class members to submit non-public, sensitive personal and financial information for purposes of employment with GE.

96. Defendants had (and continue to have) a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding and protecting their personal and financial information. Defendants also had (and continue to have) a duty to use ordinary care in activities from which harm might be reasonably anticipated (such as in the storage and protection of personal and financial information within their possession, custody and control and that of its vendors).

97. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between GE and its employees. Only Defendants were in a position to ensure that their systems were sufficient to protect against the harm to Plaintiffs and the Class members from a data breach.

98. Defendants violated these standards and duties by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' personal and financial information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the personal and financial information entrusted to it – including Plaintiffs' and Class members' personal and financial information. It was reasonably foreseeable to Defendants that their failure to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' personal and financial information by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would

result in the unauthorized release, disclosure, and dissemination of Plaintiffs' and Class members' personal and financial information.

99. Defendants, by and through their negligent actions, inaction, omissions, and want of ordinary care, unlawfully breached its duties to Plaintiffs and Class members by, among other things, failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' personal and financial information within their possession, custody and control.

100. Defendants, by and through their negligent actions, inactions, omissions, and want of ordinary care, further breached its duties to Plaintiffs and Class members by failing to design, adopt, implement, control, direct, oversee, manage, monitor and audit their processes, controls, policies, procedures, protocols, and software and hardware systems for complying with the applicable laws and safeguarding and protecting their personal and financial information.

101. But for Defendants' negligent breach of the above-described duties owed to Plaintiffs and Class members, their personal and financial information would not have been released, disclosed, and disseminated without their authorization.

102. Plaintiffs' and Class members' personal and financial information was transferred, sold, opened, viewed, mined and otherwise released, disclosed, and disseminated to unauthorized persons without their authorization as the direct and proximate result of Defendants' failure to design, adopt, implement, control, direct, oversee, manage, monitor and audit its processes, controls, policies, procedures and protocols for complying with the applicable laws and safeguarding and protecting Plaintiffs' and Class members' personal and financial information.

103. Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused this data breach constitute negligence.

104. As a direct and proximate result of Defendants' above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the data breach, Plaintiffs and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT II

NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class, Or, Alternatively, Plaintiff and the Florida Class)

105. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

106. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security to safeguard the personal and financial information of Plaintiffs and Class members.

107. The FTCA 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 the personal and financial information of Plaintiffs and Class members. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

108. Defendants required, gathered, and stored personal and financial information of Plaintiffs and Class members for employment purposes.

109. Defendants violated the FTCA by failing to use reasonable measures to protect the personal and financial information of Plaintiffs and Class members and not complying with applicable industry standards, as described herein.

110. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

111. The harm that occurred as a result of the Data Breach is the type of harm the FTCA 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 Plaintiffs and Class members.

112. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and Class members have suffered, and continue to suffer, injuries, damages arising from identify theft; from their inability to use their debit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the data breach and/or false or fraudulent charges stemming from the data breach, including but not limited to, contacting their financial institutions to dispute fraudulent charges; loss of use of funds; closing or modifying financial accounts; damages from lost time and effort to mitigate the actual and potential impact of the data breach on their lives; closely reviewing and monitoring their accounts for unauthorized activity which is certainly impending; placing credit freezes and credit alerts with credit reporting agencies; and damages from identify theft, which may take months or years to discover and detect.

113. Defendants' violation of the FTCA constitutes negligence per se.

COUNT III

BREACH OF CONTRACT

(On Behalf of Plaintiffs and the GE Employee Class Against GE)

114. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

115. Plaintiffs and Class members, upon information and belief, entered into express contracts with GE that included GE's promise to protect nonpublic personal information given to GE from disclosure.

116. Plaintiffs and Class members have performed and satisfied all of their obligations to GE, pursuant to the employment agreements, including GE's handbook titled "THE SPIRIT & THE LETTER" (the "handbook"), except those obligations they were prevented or excused from performing or satisfying.

117. GE's handbook sets the standards of conduct for its employees and GE, including protecting the privacy of GE's employees. According to GE's handbook, "[GE] respect[s] employees' privacy rights and will use, maintain and transfer personal data in accordance with GE's Employment Data Protection Standards, related procedures and local law."[28] GE is also "committed to collecting, handling and protecting Personal Information responsibly, and in compliance with applicable privacy and information security laws and with GE's Commitment to the Protection of Personal Information (GE's Binding Corporate Rules), where applicable."[29] GE defines "Personal Information" as "any information relating to a directly or indirectly identifiable person (or in some cases, a company); examples include name, address, email, phone, national identifier and credit card number."[30]

118. GE breached its contractual obligations to protect the nonpublic personal information GE possessed and was entrusted with when the information was accessed by unauthorized persons as part of the data breach.

---

[28] *See* https://www.ge.com/in/sites/www.ge.com.in/files/TheSpirit&TheLetter.pdf (last visited Apr. 17, 2020).
[29] *Id.*
[30] *Id.*

119. As a direct and proximate result of GE's above-described breach of contract, Plaintiffs and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT IV

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiffs and the GE Employee Class Against GE)

120. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

121. GE required Plaintiffs and Class members to provide their personal information, including names, addresses, Social Security numbers, financial information, the personal information of their beneficiaries and dependents, and other personal information, as a condition of their employment.

122. As a condition of Plaintiffs' and Class members' employment with GE, they provided their personal and financial information, including but not limited to the personal information of their beneficiaries and dependents. In so doing, Plaintiffs and Class members entered into implied contracts with GE by which GE agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class members if their data had been breached and compromised, or stolen.

123. Plaintiffs and Class members fully performed their obligations under the implied contracts with GE.

124. GE breached the implied contracts it made with Plaintiffs and Class members by failing to safeguard and protect their personal and financial information, including the personal information of their beneficiaries and dependents, and by failing to provide timely and accurate notice to them that personal and financial information, along with the personal information of their beneficiaries and dependents, was compromised as a result of the data breach.

125. As a direct and proximate result of GE's above-described breach of implied contract, Plaintiffs and Class members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT V

VIOLATION OF THE FLORIDA DECEPTIVE AND UNFAIR TRADE PRACTICES ACT ("FDUTPA") FLA. STAT. § 501.201 ET SEQ.

(On Behalf of Plaintiff Baz and the Florida Class)

126. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

127. FDUTPA prohibits "unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat.§ 501.204.

128. Defendants engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

129. While engaged in trade or commerce, Defendants have violated FDUTPA, including, among other things, by:

(a) failing to implement and maintain appropriate and reasonable security procedures and practices to safeguard and protect the personal and financial information of GE's current and former employees and their beneficiaries from unauthorized access and disclosure;

(b) failing to disclose that its computer systems and data security practices were inadequate to safeguard and protect the personal and financial information of GE's current and former employees and their beneficiaries from being compromised, stolen, lost, or misused; and

(c) failing to disclose the data breach to GE's current and former employees in a timely and accurate manner in violation of Fla. Stat. § 501.171.

130. Defendants knew or should have known that the Canon computer systems and data security practices were inadequate to safeguard Florida members' personal and financial information entrusted to it, and that risk of a data breach or theft was highly likely.

131. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

132. Defendants' failures constitute false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiff Baz and Florida Class members) regarding the security of Canon's network and aggregation of personal and financial information.

133. The representations upon which consumers (including Plaintiff Baz and Florida Class members) relied were material representations (e.g., as to Defendants' adequate protection

of personal and financial information), and consumers (including Plaintiff Baz and Florida Class members) relied on those representations to their detriment.

134. Defendants' actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendants engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to GE's current and former employees.

135. In committing the acts alleged above, Defendants engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to GE's current and former employees that it did not follow industry best practices for the collection, use, and storage of personal and financial information.

136. As a direct and proximate result of Defendants' conduct, Plaintiff and other members of the Class have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

137. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Florida Class members' personal and financial information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Florida Class members damages. Accordingly, Plaintiff Baz and Florida Class members are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

COUNT VI

VIOLATION OF THE NEW YORK GENERAL BUSINESS LAW § 349

(On Behalf of Plaintiffs and the Nationwide Class)

138. Plaintiffs re-allege and incorporate by reference all paragraphs as if fully set forth herein.

139. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

(a) Defendants misrepresented material facts to Plaintiffs and the Class by representing that they would maintain adequate data privacy and security practices and procedures to safeguard Class members' PFI from unauthorized disclosure, release, data breaches, and theft;

(b) Defendants misrepresented material facts to Plaintiffs and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class members' Personal Financial Information;

(c) Defendants omitted, suppressed, and concealed material facts of the inadequacy of its privacy and security protections for Class members' PFI;

(d) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class members' PFI, in violation of duties imposed by and public policies reflected in applicable federal and state laws, resulting in the data breach. These unfair acts and practices violated duties imposed by laws including the Federal Trade Commission Act (15 U.S.C. § 45);

(e) Defendants engaged in deceptive, unfair, and unlawful trade acts or practices by failing to disclose the data breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

140. Defendants knew or should have known that the Canon computer systems and data security practices were inadequate to safeguard the Class members' PFI entrusted to it, and that risk of a data breach or theft was highly likely.

141. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

142. Defendants' failure constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class members) regarding the security of Canon's network and aggregation of PFI.

143. The representations upon which consumers (including Plaintiffs and Class members) relied were material representations (e.g., as to Defendants' adequate protection of PFI), and consumers (including Plaintiffs and Class members) relied on those representations to their detriment.

144. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiffs and other Class members have been harmed, in that they were not timely notified of the data breach, which resulted in profound vulnerability to their personal information and other financial accounts.

145. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiffs' and Class members' PFI was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class members damages.

146. Plaintiffs and Class members seek relief under N.Y. Gen. Bus. Law § 349(h), including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

COUNT VII

BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiffs and All Class Members)

174. Plaintiffs re-allege and incorporate by reference all paragraphs 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 Plaintiffs' 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 Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' PII; (2) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (3) 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 Plaintiffs' 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 Plaintiffs 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 Plaintiffs 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 Plaintiffs 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 Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

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

182. As a direct and proximate result of Defendants' breaches of their fiduciary duties, Plaintiffs 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 Plaintiffs 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, Plaintiffs 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, Plaintiffs, individually and on behalf of the members of the Classes defined above, respectfully request that this Court:

A. Certify this case as a class action under Federal Rule of Civil Procedure 23, appoint Plaintiffs as the Class representatives, and appoint the undersigned as Class counsel;

B. Order appropriate relief to Plaintiffs and the Classes;

C. Enter injunctive and declaratory relief as appropriate under the applicable law;

D. Award Plaintiffs and the Classes pre-judgment and/or post-judgment interest as prescribed by law;

E. Award reasonable attorneys' fees and costs as permitted by law; and

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

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury of all claims so triable.

DATED: August 10, 2020

Respectfully submitted,

BURSOR & FISHER, P.A.

/s/ Joseph I. Marchese

Joseph I. Marchese
Philip L. Fraietta
Alec M. Leslie
888 7th Avenue
New York, NY 10019
Tel: (646) 837-7150
Fax: (212) 989-9163
Email: jmarchese@bursor.com
pfraietta@bursor.com
aleslie@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: (202) 429-2290
gklinger@masonllp.com

LEVI & KORSINSKY, LLP
Eduard Korsinsky (EK-8989)
55 Broadway, 10th Floor
New York, NY 10006
Tel: (212) 363-7500
ek@zlk.com

LEVI & KORSINSKY, LLP
Rosemary M. Rivas
388 Market Street, Suite 1300
San Francisco, CA 94111
Tel: (415) 373-1671
rrivas@zlk.com

Interim Class Counsel