UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

DIANA ROUSE, on behalf of herself and all others similarly situated,

Plaintiff,

v.

CANON U.S.A., INC.,

Defendant.

Case No. 1:21-cv-414

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff, Diana Rouse ("Plaintiff"), by and through her counsel, on her own behalf and on behalf of a class of current and former employees of Defendant Canon U.S.A., Inc. ("Canon" or "the Company"), and their beneficiaries and dependents, whose private information was compromised in the data breach disclosed by Canon in or about August of 2020 and more fully in November of 2020 (the "Canon Data Breach Class"), hereby alleges the following facts in support of her claims against Canon based upon personal knowledge, where applicable, information and belief, and the investigation of counsel:

I. INTRODUCTION

1. Canon is a provider of consumer, business-to-business, and industrial digital imaging solutions to the United States, Latin America, and the Caribbean markets. A significant portion of Canon's business products are geared towards the protection of sensitive data and documents. The Company makes it clear that, in today's often-attacked digital world, risks to computer networks come in more forms and from more directions than ever before. According to Defendant Canon's own product literature, "[f]rom identity theft and intellectual property loss to

infection by viruses and malware, IT administrators are tasked with adequately protecting information and assets from threats from the outside as well as within."[1]

2. While knowing full well that Canon's own systems were likewise subject to material security risks, including dangerous and damaging hacks and malware attacks, the Company failed to adequately protect itself and highly confidential and sensitive private information of its own current and former employees and their dependents and beneficiaries from outside cyberattack.

3. On August 4, 2020, Canon became aware of a serious ransomware attack that occurred between July 20, 2020 and August 6, 2020 on its own networks and systems. This attack resulted in an unauthorized third-party gaining access to files on Canon's servers containing fifteen years' worth of personal, sensitive and confidential information about Canon's current and former employees, and their beneficiaries and dependents, dating back to 2005.

4. To make matters worse, despite learning of the Canon Data Breach in **August 2020**, Canon did not publicly announce the Canon Data Breach until more than three months later, on or around November 25, 2020.[2] In this long delayed announcement, Canon disclosed that the data accessed by the attacker included employees' personal identifying information ("PII"), including their names, social security numbers, dates of birth, and driver's license numbers or government-issued ID numbers, as well as their personal financial information ("PFI"), including bank account numbers, and employees' electronic signatures (collectively, "Private Information"). Around the same time, Defendant notified its former employees that their Private Information had been

[1] "Device Security Overview," Canon, Inc., https://canon.a.bigcontent.io/v1/static/canon_device_security_overview (last accessed January 25, 2021).

[2] "Canon publicly confirms August ransomware attack, data theft," BleepingComputer, https://www.bleepingcomputer.com/news/security/canon-publicly-confirms-august-ransomware-attack-data-theft/ (last accessed January 25, 2021).

comprised in the Canon Data Breach and advised that their Private Information had been exposed through the ransomware attack.

5. Defendant's security failures enabled the hackers to execute the Canon Data Breach and steal Plaintiff's and Class Members' Private Information. The Canon Data Breach was caused and enabled by Defendant's violation of its obligations to abide by best practices and industry standards concerning the security of Private Information. Defendant failed to comply with security standards and allowed Plaintiff's and the Class Members' Private Information to be compromised by failing to prevent and mitigate the Canon Data Breach that occurred.

6. Plaintiff Diana Rouse was employed by Canon for several years until she left the Company in 2005. As a condition of her employment, Ms. Rouse was required to and did provide her personal identifying and financial information to Canon, including the very type of Private Information stolen by the criminals during the Canon Data Breach. In addition, during the course of her employment by Canon, Plaintiff Rouse was required to provide account information for her personal credit card account, which Canon kept on file, to make employment-related purchases that she was subsequently reimbursed for by Canon.

7. Plaintiff entrusted this confidential information about herself and her family to Canon's care. Canon, however, betrayed that trust and unlawfully allowed Plaintiff's Private Information, to be accessed and stolen by unauthorized third-parties without her knowledge or consent.

8. Plaintiff Rouse brings this class action on behalf of herself and the Canon Data Breach Class based on Canon's failure to properly protect its employees' highly sensitive personal and financial information, including employees' names, social security numbers, dates of birth,

numbers for driver's licenses or government-issued IDs, bank account numbers utilized for direct deposits from Canon, and electronic signatures (among others).

9. Plaintiff and the Canon Data Breach Class members have been exposed to a heightened and imminent risk of fraud and identity theft, including the imminent and impending injury flowing from potential fraud and identify theft posed by their bank account and personal information being placed in the hands of criminals and the risk of misuse via the sale of Plaintiff's and Canon Data Breach Class Members' Private Information on the Internet black market. As such, Canon Data Breach Class Members must now and in the future (as there is little ability to predict when the stolen data may be used) closely monitor their financial accounts to guard against fraud and maintenance of their privacy.

10. Accordingly, Plaintiff, on behalf of herself and other members of the Canon Data Breach Class, asserts claims for negligence, negligence *per se*, unjust enrichment, breach of implied contract, and violation of California's Unfair Competition Law, seeking monetary damages, statutory damages, injunctive relief, and all other relief as authorized in equity or by law. Specifically, Plaintiff seeks remedies including reimbursement of losses and other out-of-pocket costs, compensation for time spent in response to the Canon Data Breach, and free credit monitoring and identity theft insurance, beyond the inadequate one-year offered by Canon.

Parties

Plaintiff Diana Rouse

11. Plaintiff Diana Rouse is a citizen and resident of the State of California, residing at 14311 Heatherfield Drive, Tustin, CA 92780.

12. Plaintiff Rouse received a Notice of Data Breach Letter from Canon notifying her that her Private Information was accessed without authorization. The letter was dated November 24, 2020.

13. In addition to privacy-related harms stemming from Defendant's collection and storage of Plaintiff's Private Information, Plaintiff Rouse suffered actual injury in the form of damages to and diminution in the value of her Private Information, a form of intangible property that she entrusted to Defendant for the purpose of her employment, which was compromised as a result of the Canon Data Breach. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft, and misuse posed by her Private Information being placed in the hands of criminals. Since the Canon Data Breach, Plaintiff Rouse has experienced an avalanche of scam phone calls purportedly designed to obtain additional personal data to commit identify theft by way of social engineering attack and other nefarious means. The uptick in spam calls since the Canon Data Breach has been significant and disruptive to her daily life.

14. Upon information and belief, Plaintiff's Private Information has been made available to unauthorized third-parties, including through the dark web, as a result of the Canon Data Breach.

15. Plaintiff and the Class Members have a continuing interest in ensuring that their Private Information is protected and safeguarded from future breaches.

16. The injuries suffered by Plaintiff and the Canon Data Breach Class members as a direct result of the Canon Data Breach include one or more of the following:

a. unauthorized use of their Private Information;

b. theft of their Private Information;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their Private Information;

e. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Canon Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Canon Data Breach (which time spent on those activities Plaintiff and the Canon Data Breach Class Members could have been working and earning a living, therefore suffering further actual injury);

f. the imminent and impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

g. damages to and diminution in value of their Private Information entrusted to Defendant for the purpose of their employment by Defendant; and

h. the loss of Plaintiff's and the Canon Data Breach Class Members' privacy.

Defendant Canon U.S.A., Inc.

17. Defendant Canon U.S.A., Inc. is a New York corporation with its principal place of business located at One Canon Park, Melville, New York 12207. It is a citizen of the State of New York.

18. Canon emphasizes and takes pride in its products and its ability to protect privacy of product users, but yet Canon fails to adequately protect the privacy rights of its own employees.

19. As discussed more fully below, Canon makes significant profits at the expense of its hard-working current and former employees. Trust and loyalty have a price at Canon, a price

the Company is not willing to pay. Instead, Canon betrayed the trust of its employees by willfully putting at risk of attack by cybercriminals their Private Information. Canon chose to maintain inadequate information technology systems, exposing its employees' Private Information, including highly sensitive social security numbers, birth dates, driver's license numbers, and bank account information, to cyberattack. Through this lawsuit, the thousands of affected Canon employees have a voice in Plaintiff Rouse.

Jurisdiction and Venue

20. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d)(2), because at least one Class Member (Plaintiff Rouse) is of diverse state citizenship from Defendant, there are more than 100 Class Members, and the aggregate amount in controversy exceeds $5 million, exclusive of interest and costs.

21. The Eastern District of New York has personal jurisdiction over Defendant as it is incorporated in this State. In addition, Defendant is headquartered in this District, and conducts substantial business in this State and in this District through its headquarters, sale of products, and commercial website and the storage of data and information subject to the Canon Data Breach.

22. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant has its principal place of business in this District and because a substantial part of the events or omissions giving rise to the conduct alleged in this Complaint occurred in, were directed to, and were emanated from this District.

II. FACTUAL ALLEGATIONS

The Canon Data Breach

23. On or about August 4, 2020, Canon learned of a ransomware attack that occurred between July 20, 2020 and August 6, 2020 on its networks and file systems, which resulted in an

unauthorized third-party gaining access to files on its servers that contained personal and confidential information about Canon's current and former employees who were employed from 2005 to 2020, as well as their beneficiaries and dependents.

24. On August 13, 2020, Canon posted this, uninformative notice on its corporate website a "Cybersecurity Notice for Canon Websites" that stated:

> Canon U.S.A., Inc. and its subsidiaries understand the importance of maintaining the operational integrity and security of our systems. Access to some Canon systems is currently unavailable as a result of a ransomware security incident we recently discovered.
>
> We immediately implemented our response protocols and began an investigation. Cybersecurity experts who have worked with other companies that have had similar issues, have been engaged. We are working quickly to address the issue and to restore operations. We appreciate your patience as we work through this incident. Thank you.

25. On information and belief, on or around August 6, 2020, Canon sent a company-wide notification entitled "Message from IT Service Center" that was sent from Canon's IT department. The notification stated:

> Attention: Canon USA is experiencing widespread system issues, affecting multiple applications, Teams, Email and other systems may not be available at this time. We apologize for the inconvenience – a status update will be provided as soon as possible.

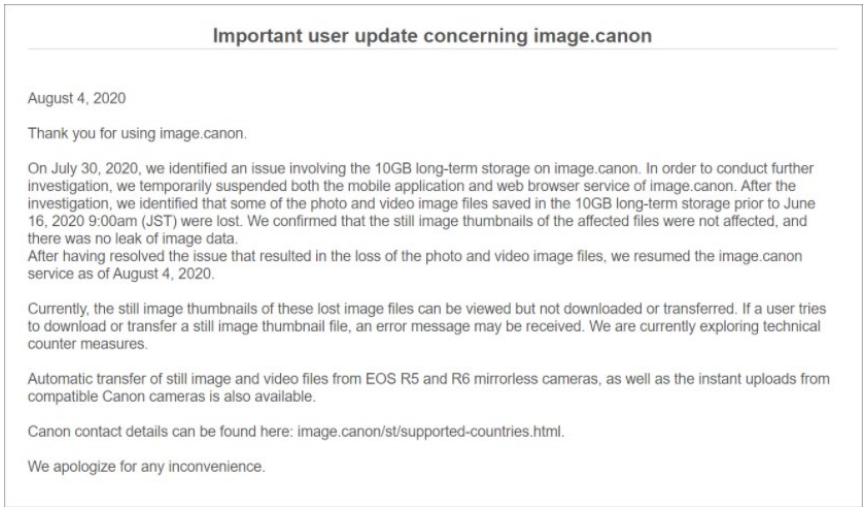
26. Despite learning of the Canon Data Breach in August 2020, Canon initially downplayed the significance of the breach and did not publicly announce the Canon Data Breach until November 25, 2020, at which time Canon disclosed that the data accessed by the attacker included employees' names, social security numbers, dates of birth, driver's license numbers or government-issued ID numbers, bank account numbers, and their electronic signatures.[3]

[3] "Canon publicly confirms August ransomware attack, data theft," BleepingComputer, https://www.bleepingcomputer.com/news/security/canon-publicly-confirms-august-ransomware-attack-data-theft/ (last accessed January 25, 2021).

27. Canon, however, failed to notify its former employees of the Canon Data Breach, including the fact that their Private Information had been compromised in the Canon Data Breach, until late November of 2020, over three and a half months after the breach occurred and was discovered by Canon.

Canon's Data Security Standards were Inadequate

28. Defendant was on notice of the very real risks of security breaches like the Canon Data Breach. In information and belief, Canon suffered several data breaches in 2020, the most recent being an unrelated data breach of its computer systems in July of 2020, when the image.canon site suffered an outage. Canon released the following user notice[4] related to that security breach:



Important user update concerning image.canon

August 4, 2020

Thank you for using image.canon.

On July 30, 2020, we identified an issue involving the 10GB long-term storage on image.canon. In order to conduct further investigation, we temporarily suspended both the mobile application and web browser service of image.canon. After the investigation, we identified that some of the photo and video image files saved in the 10GB long-term storage prior to June 16, 2020 9:00am (JST) were lost. We confirmed that the still image thumbnails of the affected files were not affected, and there was no leak of image data.
After having resolved the issue that resulted in the loss of the photo and video image files, we resumed the image.canon service as of August 4, 2020.

Currently, the still image thumbnails of these lost image files can be viewed but not downloaded or transferred. If a user tries to download or transfer a still image thumbnail file, an error message may be received. We are currently exploring technical counter measures.

Automatic transfer of still image and video files from EOS R5 and R6 mirrorless cameras, as well as the instant uploads from compatible Canon cameras is also available.

Canon contact details can be found here: image.canon/st/supported-countries.html.

We apologize for any inconvenience.

29. Security breaches like the Canon Data Breach have been frequent and garnered significant media attention over the last decade, with significant data breaches dating back to 2005. The Privacy Rights Clearinghouse, a nonprofit organization which focuses on strengthening

[4] "Canon confirms ransomware attack in internal memo", BleepingComputer, https://www.bleepingcomputer.com/news/security/canon-confirms-ransomware-attack-in-internal-memo/ (last visited January 25, 2021).

privacy protections, has recorded over 9,000 data-related security breaches in the U.S. since 2005, including numerous instances of hacking.[5]

30. Despite the known risk of a data breach and widespread publicity and industry alerts regarding other notable data breaches, Canon failed to take reasonable steps to adequately protect its computer systems from being breached and failed to protect its own employees' sensitive personal information entrusted to it. Canon could have prevented the breach and more timely notified affected individuals by ensuring that their systems established and maintained adequate security protocols that safeguarded against cyberattacks.

31. Defendant should have been well-aware of the risk of falling victim to a data breach, given its prior breach history, and should have taken adequate steps to secure against such an attack.

32. Plaintiff and other Class Members relied on Defendant to have implemented and maintained adequate systems that would keep their Private Information safe, as Defendant had a duty to keep its employees' Private Information safe. Defendant failed to comply with this duty.

Defendant Failed to Comply with Industry Standards

33. Federal and State governments have established security standards and issued recommendations to temper data breaches and the resulting harm to consumers and financial institutions. The Federal Trade Commission ("FTC") has issued numerous guides for businesses, highlighting the importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

34. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which establishes guidelines for fundamental data security principles and practices

[5] Data Breaches, Privacy Rights Clearinghouse, https://privacyrights.org/data-breaches (last visited January 25, 2021).

for business. The guidelines note 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; keep software updated; and implement policies to correct 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.

35. The FTC recommends that businesses limit who can access sensitive data; require complex passwords to be used on networks; use industry-tested methods to ensure security and avoid hacking; monitor for suspicious activity on the network; ensure coding in software used by the business is secure; test systems for common security vulnerabilities and verify that third-party service providers have implemented reasonable security measures.

36. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect 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.

37. Despite Defendant's awareness of its data security obligations and its promises to customers that their personal data would be secured and protected, Defendant's treatment of Private Information entrusted to it by its employees fell far short of satisfying Defendant's legal duties and obligations. Defendant failed to ensure that access to its data systems was reasonably

safeguarded, failed to follow industry standards for the protection of Private Information and failed to use proper security systems to detect and deter the type of attack that occurred and is at issue here.

38. As a result of Defendant's failure to adhere to industry and government standards for the security of Private Information of thousands of Defendant's current and former employees, including Plaintiff and Canon Data Breach Class Members, was compromised.

39. Canon is, and at all relevant times has been, aware that the Private Information it maintains on its employees and their beneficiaries and dependents is highly sensitive and could be used for nefarious purposes by third-parties, such as perpetrating identity theft, making fraudulent purchases, and/or fraudulent accessing of individuals' bank accounts.

40. Canon understands the importance of adequately safeguarding its employees' and their beneficiaries' and dependents' sensitive personal and bank account information. Despite Canon recognizing the importance of its employees' and their beneficiaries' and dependents' privacy, and other than the on-line notice, Canon failed to adequately safeguard the Class Members' Private Information, or otherwise, prevent and mitigate the Canon Data Breach that occurred.

41. Canon is thus aware of the importance of safeguarding its employees' and their beneficiaries' and dependents' personal and bank account information from the foreseeable consequences that would occur if its data security systems were breached.

42. Because Canon required Plaintiff and other Canon employees to provide their Private Information as a condition of their employment at Canon, Canon had a legal duty to protect the private, highly sensitive, and confidential Private Information of Plaintiff and the members of the Canon Data Breach Class.

43. Defendant Canon failed to safeguard and prevent the theft of this Private Information from its computers or network. It failed to take reasonable precautions to protect the Private Information of Plaintiff and the Canon Data Breach Class, and otherwise failed to act reasonably in fulfillment of its duty to current and former employees, and their beneficiaries and dependents.

44. The attackers maintained access to the Canon file systems from July 20, 2020 to August 6, 2020. The breach of Canon's computer systems, and the compromise of its employee Private Information, including highly sensitive social security numbers, birth dates, and sensitive bank information, was the direct and proximate result of Canon's inadequate security measures.

45. As a result, Plaintiff and members of the Canon Data Breach Class have suffered and will continue to suffer damages from the loss of access to and use of the existing credit, the compromise and use of such existing credit, the unauthorized opening of new credit accounts and use of such new credit, and the opening of other accounts in their name. There is also the very real potential for the cyber criminals to file false tax returns this year (as typically happens in such cases) to fraudulently collect refunds, which refunds belong to members of the Canon Data Breach Class.

Security Breaches Lead to Identity Theft

46. According to the U.S. Department of Justice Bureau of Justice Statistics, an estimated 26 million people were victims of one or more incidents of identity theft in 2016. Among identity theft victims, existing bank or credit accounts were the most common types of misused information.

47. Similarly, the FTC cautions that identity theft wreaks havoc on individuals' finances, credit history, and reputation and can take time, money, and patience to resolve. Identity

thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

48. Private Information—which includes Plaintiff's and Class Members' names and social security numbers combined with their bank account information that were stolen in the Canon Data Breach—is a valuable commodity to identity thieves. At all relevant times, Defendant was well-aware, or reasonably should have been aware, that the Private Information disclosed by employees and stored on the file servers and systems that Defendant operates is highly sensitive and could be used for wrongful purposes by third-parties, such as identity theft and fraud.

49. Stolen Private Information is a valuable commodity. A "cyber black-market" on the dark web exists, in which criminals openly post stolen payment card numbers, social security numbers, and other personal information on a number of underground Internet websites. Identity thieves use stolen Private Information to open new financial accounts to take out loans in another person's name, incur charges on existing accounts, or clone ATM, debit, or credit cards. Stolen Private Information may be traded on the dark web for years.

50. The growing sophistication of hackers to commit identity theft and fraud are of serious concern and directly implicated in the Canon Data Breach. Hackers are able to gain access to a wide variety of an individual's personal accounts through minimal information. For example, "a billing address and the last four digits of a credit card number are the only two pieces of information anyone needs to get into your iCloud account." From there, "hackers were able to […] take over all of [an individual's] digital devices – and data." Further, hackers have the capability to generate a CVV code "starting with no details at all other than the first six digits" of a payment card, thereby enabling "hackers [to] obtain the three essential pieces of information to make an online purchase within as little as six seconds."

51. The National Institute of Standards and Technology categorizes the combination of names and credit card numbers as sensitive and warranting a higher impact level based on the potential harm when used in contexts other than their intended use. Private Information that is "linked" or "linkable" is also more sensitive. Linked information is information about or related to an individual that is logically associated with other information about the individual. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual. An example of linking information the NIST report cites is a Massachusetts Institute of Technology study showing that 97% of the names and addresses on a voting list were identifiable using only ZIP code and date of birth.

52. Private Information is broader in scope than directly identifiable information. As technology advances, computer programs become increasingly able to scan the Internet with wider scope to create a mosaic of information that may be used to link information to an individual in ways that were not previously possible.

Damages Sustained by Plaintiff and Class Members

53. Plaintiff and the other members of the Canon Data Breach Class have suffered injury and damages, including, but not limited to one or more of the following:

a. Defendant's unauthorized and undisclosed collection of their Private Information;

b. unauthorized use of their Private Information;

c. theft of their Private Information;

d. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

e. damages arising from the inability to use their Private Information;

f. Time spent and costs associated with the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Canon Data Breach, and the stress, nuisance and annoyance of dealing with all issues resulting from the Canon Data Breach (which time spent on those activities Plaintiff and the Canon Data Breach Class members could have been working and earning a living, therefore suffering further actual injury);

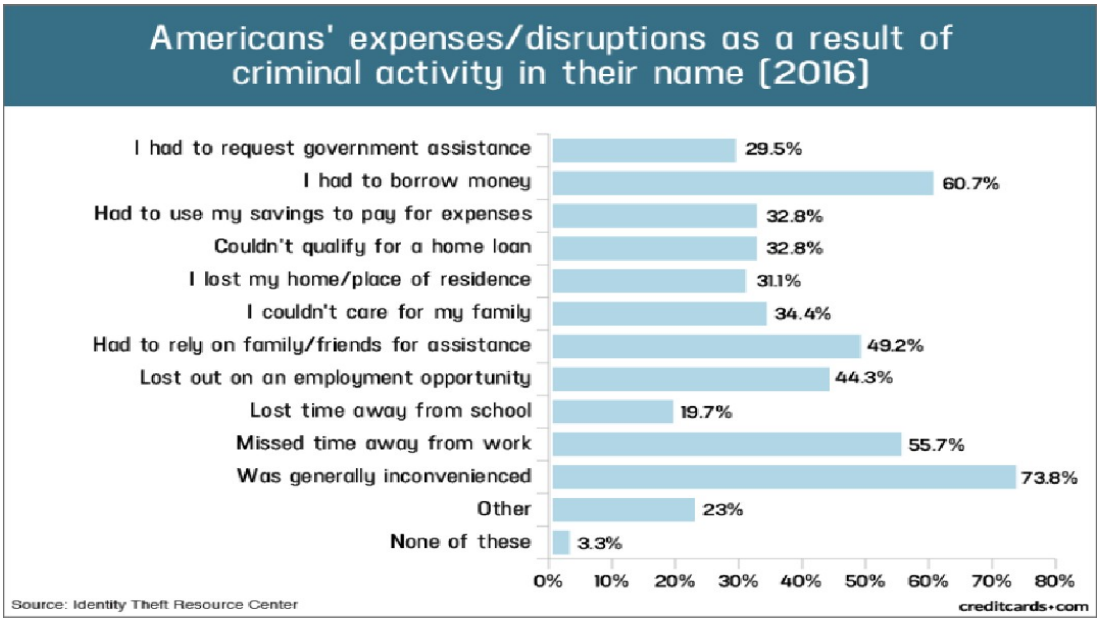
g. the imminent and impending injury flowing from potential fraud and identity theft posed by their Private Information being placed in the hands of criminals;

h. damages to and diminution in value of their Private Information entrusted to Defendant; and

i. the loss of Plaintiff's and Canon Data Breach Class Members' privacy.

54. A study by the Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal information:[6]

[6] Jason Steele, Credit Card and ID Theft Statistics (Oct. 24, 2017) available at https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php (last visited January 25, 2021).



III. CLASS ACTION ALLEGATIONS

55. Pursuant to the provisions of Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure, Plaintiff brings this action on behalf of herself and all other current and former employees of Canon, and their beneficiaries and dependents, similarly situated in the states in which they reside, as a member of the following proposed Canon Data Breach Class:

> **All current and former employees of Canon, and their beneficiaries and dependents, whose Private Information was compromised in the data breach disclosed by Canon in or about August of 2020 and more fully in November of 2020. Excluded from the Class are Defendant, any entity in which a Defendant has a controlling interest, and their legal representatives, heirs, successors, and any governmental entities.**

56. In addition, Plaintiff seeks to represent a subclass composed of California residents (the "California Subclass"), defined as follows:

> **All current and former employees of Canon who reside in California, and their beneficiaries and dependents who reside in California, and whose Private Information was compromised in the data breach disclosed by Canon in or about August of 2020 and more fully in November of 2020. Excluded from the Class are Defendant, any entity in which a Defendant has a controlling interest, and their legal representatives, heirs, successors, and any governmental entities.**

57. Certification of Plaintiff's claims for Class-wide treatment is appropriate because all elements of Fed. R. Civ. P. 23(a), (b)(2)-(3) are satisfied. Plaintiff can prove the elements of her claims on a Class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

58. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(l) are satisfied. The members of the Canon Data Breach Class are so numerous and geographically dispersed that individual joinder of all Canon Data Breach Class members is impracticable. While Plaintiff is informed and believes that there are thousands of members of the Canon Data Breach Class, the precise number of Canon Data Breach Class members is unknown to Plaintiff. Plaintiff believes that the identity of Canon Data Breach Class members is known or knowable by Canon. Class members may be identified through objective means. Canon Data Breach 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.

59. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Canon Data Breach Class members, including, without limitation:

a. whether Defendant engaged in the active misfeasance and misconduct alleged herein;

b. whether Canon owed a duty to Plaintiff and members of the Canon Data Breach Class to act reasonably to protect their Private Information, including social security numbers and bank account information;

c. whether Canon failed to provide adequate security to protect its current and former employees' Private Information, including bank account information;

d. whether Plaintiff and the Canon Data Breach Class members are at an increased risk for identity theft because of the Canon Data Breach;

e. whether Defendant's conduct violated Cal. Bus. & Prof. Code § 17200, *et seq.*;

f. whether Canon negligently, or otherwise improperly, allowed third-parties to access its current and former employees' Private Information, including social security numbers and bank account information;

g. whether Plaintiff and members of the Canon Data Breach Class were injured and suffered damages and ascertainable losses;

h. whether Canon's failure to provide adequate security proximately caused Plaintiff's and Canon Data Breach Class members' injuries; and

i. whether Plaintiff and members of the Canon Data Breach Class are entitled to damages and, if so, the measure of such damages.

60. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Canon Data Breach Class, having provided her Private Information and had her Private Information compromised in the Canon Data Breach. Plaintiff's claims are typical of the other Canon Data Breach Class Members' claims because, among other things, all Canon Data Breach Class members were comparably injured through Defendant's conduct.

61. **Adequacy of Representation:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Canon Data Breach Class representative because she is a member of the Canon Data Breach Class and her interests do not conflict with the interests of the other members of the Canon Data Breach Class that she seeks to represent. Plaintiff is committed to

pursuing this matter for the Canon Data Breach Class with the Canon Data Breach Class's collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type and Plaintiff intends to prosecute this action vigorously. Plaintiff, and her counsel, will fairly and adequately protect the Canon Data Breach Class's interests.

62. **Predominance and Superiority:** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's individual case will also resolve them for the Canon Data Breach Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Canon Data Breach Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendant, so it would be impracticable for members of the Canon Data Breach Class to individually seek redress for Defendant's wrongful conduct. Even if Canon Data Breach Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

63. **Cohesiveness:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendant has acted, or refused to act, on grounds generally applicable to the Canon Data Breach Class making final declaratory or injunctive relief appropriate.

IV. CAUSES OF ACTION

COUNT I
NEGLIGENCE
(On Behalf of Plaintiff and the Canon Data Breach Class)

64. Plaintiff hereby incorporates by reference the allegations of paragraphs 1 through 63 above as if fully set forth herein.

65. Canon owed, and continues to owe, a duty of care to Plaintiff and the Canon Data Breach Class to do all of the following: (1) ensure that employee and Class Members' Private Information was secure; (2) ensure that employee and Class Members' Private Information was not compromised or accessed by anyone for an improper purpose without consent by Plaintiff and the Canon Data Breach Class; and (3) ensure employee and Class Members' Private Information was not used for improper purposes. This duty of care also included a duty of reasonable care in safeguarding employee and Class Members' Private Information and discovering any breach in a timely manner, and then timely reporting such breach to affected employees.

66. Canon breached its duty of care to Plaintiff and the Canon Data Breach Class by failing to provide adequate protections to the Private Information and by allowing the Private Information to be accessed by third-parties, including cyber hackers. Canon breached its duty of care by failing to timely discover the breach of employee and Class Members' Private Information and failing to timely report such breach to affected employees, like Plaintiff Rouse.

67. As a direct and proximate result of the Defendant's actions alleged above, the Plaintiff and the Canon Data Breach Class suffered damages, including the loss of time and money expended to mitigate the damages of the Canon Data Breach, out of pocket expenditures, as well as the loss of money in the future, the loss and value of time spent in seeking to resolve the problems caused by the theft of the Class Members' identity, and the loss of credit.

68. In breaching its duty to Plaintiff and the Class, Canon acted wantonly, recklessly and with utter disregard for the impact of their negligent conduct on affected Canon employees, like Ms. Rouse.

WHEREFORE, Plaintiff, on behalf of herself and the members of the Canon Data Breach Class, respectfully seeks the relief set forth below.

COUNT II
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Canon Data Breach Class)

69. Plaintiff hereby incorporates by reference the allegations of paragraphs 1 through 63 above as if fully set forth herein.

70. Various statutes, laws and regulations define the nature and scope of appropriate conduct in relation to cybersecurity. These statutes, laws and regulations are applicable to Defendant Canon and governed its conduct.

71. By its acts and omissions set forth herein, Defendant Canon breached and violated these statutes, laws, and regulations.

72. As a direct and proximate result of such breaches and violations of statutes, laws and regulations, Canon caused harm to Plaintiff and the Canon Data Breach Class as detailed herein.

73. Plaintiff and the Class have suffered, and will continue to suffer, harm due to the negligence *per se* of Defendant Canon.

WHEREFORE, Plaintiff, on behalf of herself and the members of the Canon Data Breach Class, respectfully seeks the relief set forth below.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Canon Data Breach Class)

74. Plaintiff hereby incorporates by reference the allegations of paragraphs 1 through 63 above as if fully set forth herein.

75. As a condition to their employment, Plaintiff and the Canon Data Breach Class were required to and did provide their Private Information to Canon, including the very type of Private Information stolen by the criminals during the Canon Data Breach.

76. Canon required and obtained the Private Information of Plaintiff and the members of the Canon Data Breach Class as part of the employment relationship.

77. Canon had a legal duty to protect the private, highly sensitive, and confidential Private Information of Plaintiff and the members of the Canon Data Breach Class, and to act reasonably to keep its employees,' and their beneficiaries' and dependents,' Private Information safe.

78. Plaintiff and members of the Canon Data Breach Class performed services as employees of Canon in good faith and under the assumption that Canon was appropriately safeguarding their Private Information, which had been entrusted to Canon.

79. Canon accepted the services rendered by Plaintiff and the Canon Data Breach Class but failed to adequately protect the highly sensitive information provided to it by its own employees. To the extent that Canon stored Private Information pertaining to former employees, Canon had a duty to protect that information from unauthorized exposure.

80. Canon breached its legal duty to protect the private, highly sensitive, and confidential Private Information of Plaintiff and the members of the Canon Data Breach Class.

81. As a proximate result of Canon's breach of contract, Plaintiff and the members of the Canon Data Breach Class have been injured and harmed.

WHEREFORE, Plaintiff, on behalf of herself and the members of the Canon Data Breach Class, respectfully seeks the relief set forth below.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiff and the Canon Data Breach Class)

82. Plaintiff hereby incorporates by reference the allegations of paragraphs 1 through 63 above as if fully set forth herein.

83. By engaging in the conduct described in this Complaint, Defendant has knowingly obtained benefits from Plaintiff and the Canon Data Breach Class, namely their labor and the profits therefrom, and actual monies and other benefits under circumstances such that it would be inequitable and unjust for Defendant to retain them.

84. By engaging in the acts and failures to act described in this Complaint, Defendant Canon has been knowingly enriched by the savings in costs that should have been reasonably expended to protect the Private Information of its employees, including the Plaintiff and the Canon Data Breach Class. Defendant Canon knew or should have known that theft of the Private Information within its possession could happen, yet it failed to take reasonable steps to pay for the level of security required to have prevented the theft of Private Information of Plaintiff and the Canon Data Breach Class.

85. Defendant would be unjustly enriched if it was permitted to retain the benefits derived from the exposure and potential theft of Plaintiff's and the Canon Data Breach Class's Private Information.

86. Plaintiff and each member of the Canon Data Breach Class are therefore entitled to an award of compensatory damages in an amount to be determined at trial, or the imposition of a constructive trust upon the monies derived by the Defendant by means of the above-described actions.

WHEREFORE, Plaintiff, on behalf of herself and the members of the Canon Data Breach Class, respectfully seeks the relief set forth below.

COUNT V
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE §17200, *et seq.* – UNLAWFUL BUSINESS PRACTICES
(On Behalf of Plaintiff and the Canon Data Breach Class, or in the Alternative, On Behalf of the California Subclass)

87. Plaintiff hereby incorporates by reference the allegations of paragraphs 1 through 63 above as if fully set forth herein.

88. Canon's business practices as complained of herein violate California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq*. (the "UCL").

89. In violation of the UCL, Canon has engaged in unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof. Code § 17200.

90. Specifically, Canon engaged in unlawful acts and practices by failing to establish adequate security practices and procedures as set forth above, by soliciting and gathering Plaintiff's and California Subclass Members' Private Information knowing that the information would not be adequately protected, and by storing Plaintiff's and California Subclass Members' Private Information in an unsecure electronic system in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Canon to undertake reasonable measures to safeguard the Private Information of Plaintiff and the California Subclass Members.

91. Canon's actions and practices are "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiff and the California Subclass outweighs the utility of Canon's conduct. This conduct includes Canon's failure to adequately ensure the privacy, confidentiality, and security of members' data entrusted to it and Canon's failure to have adequate data security measures in place.

92. In addition, Canon engaged in unlawful acts and practices by failing to timely and accurately disclose the data breach to California Subclass Members, in violation of the duties imposed by Cal. Civ. Code § 1798.82.

93. Canon knew or should have known that its data security practices with respect to its computer systems were inadequate to safeguard California Subclass Members' Private Information, and that as a result, the risk of a data breach or theft was highly likely. Defendant's unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiff and the California Subclass Members.

94. As a direct and proximate result of Canon's unlawful acts and practices, Plaintiff and members of the California Subclass suffered injury in fact and lost money or property, including but not limited to the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described above.

95. In addition, Plaintiff and the California Subclass Members have and will continue to incur economic damages related to the Canon Data Breach, including loss of time and money spent remedying the Data Breach, and the costs of credit monitoring, purchasing credit reports, and implementing credit freezes to prevent opening of unauthorized account, among others.

96. Accordingly, Plaintiff and the California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the California Subclass Members of money or property that Canon acquired by means of its unlawful and unfair business practices, disgorgement of all profits Canon received as a result of its unlawful and unfair business practices, declaratory relief, attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5, and injunctive or other equitable relief.

WHEREFORE, Plaintiff, on behalf of herself and the members of the Canon Data Breach Class, which includes the California Subclass, respectfully seeks the relief set forth below.

COUNT VI
VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW
CAL. BUS. & PROF. CODE §17200, *et seq*. – UNFAIR BUSINESS PRACTICES
(On Behalf of Plaintiff and the Canon Data Breach Class,
Or in the Alternative, On Behalf of the California Class)

97. Plaintiff hereby incorporates by reference the allegations of paragraphs 1 through 63 above as if fully set forth herein.

98. Canon's practices as complained of herein violate California's UCL.

99. Specifically, Canon engaged in unfair acts and practices by failing to establish adequate security practices and procedures, by soliciting and collecting Plaintiff's and California Subclass Members' Private Information knowing that the information would not be adequately protected, and by storing Plaintiff's and California Subclass Members' Private Information in an unsecure electronic system. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or damaging to Plaintiff and California Subclass Members, as they were likely to deceive California Subclass Members into believing their Private Information was securely stored when it was not.

100. Canon's actions and practices constitute "unfair" business practices in violation of the UCL, because, among other things, the gravity of the harm to Plaintiff and the California Subclass outweighs the utility of Canon's conduct. This conduct includes Canon's failure to adequately ensure the privacy, confidentiality, and security of members' data entrusted to it and Canon's failure to have adequate data security measures in place.

101. Specifically, Canon engaged in unfair acts and practices by failing to take appropriate action following the data breach to mitigate the effects of the Canon Data Breach, enact adequate privacy and security measures, and protect Plaintiff's and California Subclass Members' Private Information from further unauthorized disclosure, release, data breaches, and theft. These unfair acts and practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and damaging to Plaintiff and California Subclass Members.

102. As a direct and proximate result of Canon's acts of unfair practices and acts, Plaintiff and the California Subclass Members were injured and lost money or property, including but not limited to the loss of California Subclass Members' legally protected interest in the confidentiality and privacy of their Private Information, nominal damages, and additional losses as described above.

103. Canon knew or should have known that its computer systems and data security practices were inadequate to safeguard California Subclass Members' Private Information and that the risk of a data breach or theft was highly likely. Canon's actions in engaging in the above-named unlawful practices and acts were negligent, knowing and willful, and/or wanton and reckless with respect to the rights of members of the California Subclass.

104. Accordingly, Plaintiff and the California Subclass Members seek relief under Cal. Bus. & Prof. Code § 17200, *et seq*., including, but not limited to, restitution to Plaintiff and the

California Subclass Members of money or property that Canon may have acquired by means of its unfair business practices, disgorgement of all profits accruing to Canon because of its unfair business practices, declaratory relief, attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5, and injunctive or other equitable relief.

105. Plaintiff and the California Subclass members reserve the right to amend this Complaint as of right to seek damages and relief under Cal. Civ. Code § 1798.100, *et seq*.

WHEREFORE, Plaintiff, on behalf of herself and the members of the Canon Data Breach Class, which includes the California Subclass, respectfully seeks the relief set forth below.

V. REQUEST FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Canon Data Breach Class, respectfully requests that the Court:

a) Certify the California Data Breach Class, including the California Subclass, and appoint Plaintiff Rouse and her counsel to represent the California Data Breach Class, which includes the California Subclass;

b) Finding that Defendant engaged in the unlawful conduct as alleged herein;

c) Enter a monetary judgment in favor of Plaintiff and the Canon Data Breach Class, including the California Subclass, to compensate them for the injuries suffered, together with pre-judgment and post-judgment interest, treble damages, and penalties where appropriate;

d) Require Defendant to rectify all damages caused by its misconduct;

e) Award Plaintiff and the Canon Data Breach Class, including the California Subclass, reasonable attorneys' fees and costs of suit, as allowed by law; and

f) Award such other and further relief as this Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: January 25, 2020

Respectfully submitted,

/s/ Lori G. Feldman
Lori G. Feldman, Esq.
GEORGE GESTEN MCDONALD, PLLC
102 Half Moon Bay Drive
Croton-on-Hudson, New York 10520
Phone: (917) 983-9321
Fax: (888) 421-4173
Email: LFeldman@4-justice.com
E-Service: eService@4-Justice.com

David J. George, Esq.
Brittany L. Brown, Esq.
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Phone: (561) 232-6002
Fax: (888) 421-4173
Email: DGeorge@4-Justice.com
E-Service: eService@4-Justice.com