JUDGE RICHARD A. JONES

UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

AT SEATTLE

IN RE: FORTIVE DATA SECURITY LITIGATION **THIS DOCUMENT RELATES TO:** All Actions	CASE NO. 2:24−CV−01668−RAJ

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Michael Dudley and Sherry Dudley, Matthew Spaeth, Jennifer Nelson, Seth Toepfer and Marilyn Cazares f/k/a Marilyn Mews, (collectively "Plaintiffs") bring this Class Action Complaint on behalf of themselves and all others similarly situated, against Defendant Fortive Corporation ("Fortive"), Accruent LLC ("Accruent"), Advanced Sterilization Product Services Inc., and Advanced Sterilization Products, Inc., (together "ASPS"), Censis Technologies Inc., ("Censis") and Industrial Scientific Corporation d/b/a Industrial Scientific Devices, ("Industrial Scientific") (collectively, "Defendants") and allege as follows, based upon information and belief and investigation of counsel, except as to the allegations specifically pertaining to Plaintiffs, which are based on personal knowledge:

1. Entities that gather and retain sensitive, personally identifying information ("PII" or "Private Information") owe a duty to the individuals to whom that data relates. This duty arises

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

because it is foreseeable that the exposure of consumers' PII to unauthorized persons—especially hackers with nefarious intentions—will cause harm to such individuals.

2. Defendant Fortive represents itself as a "provider of essential technologies for connected workflow solutions across a range of attractive end-markets."[1] Fortive maintains operations in multiple market segments including Intelligent Operating Solutions, Precision Technologies, and Advanced Healthcare Solutions. Defendant Fortive also owns subsidiaries including Accruent, Advanced Sterilization Products, Censis Technologies, Inc., Fluke Corp., Industrial Scientific Corporation, Pacific Scientific Energetic Materials, Setra Systems, Inc., and The Gordian Group, Inc., all of which were affected by the data breach as alleged herein.

3. In the course of its business, Defendant Fortive, along with its subsidiaries, including Defendants Accruent and ASPS, collects consumer data including, but not necessarily limited to, employees and consumers' social security numbers, first and last names, dates of birth, full addresses, and preferred mailing addresses, and has a resulting duty to securely maintain such information in confidence.

4. Defendant Fortive warrants to employees and consumers that the services it offers on its website are safe and secure. For example, it represents:

> We implement and maintain reasonable security appropriate to the nature of the Personal Information that we collect, use, retain, transfer or otherwise process. Our reasonable security program is implemented and maintained in accordance with applicable law and relevant standards as outlined in the report issued by the California Attorney General in February 2016.[2]

5. Additionally, its subsidiary: Advanced Sterilization Products, Inc. represents:

> We ensure the security of your personal data by processing it in accordance with appropriate technical and organizational measures. We also take steps to ensure all our subsidiaries, agents, affiliates and suppliers employ adequate levels of security.[3]

---

[1] https://investors.fortive.com/company-information
[2] Fortive Corp CCPA Public Facing Privacy Notice (20191218bis)
[3] ASPS, Privacy Policy, https://www.asp.com/en-us/privacy-notice#wheredowe (last visited October 24, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

6. Contrary to its assurances, Defendants did not maintain adequate systems and procedures to ensure the security of the highly sensitive PII its employees and consumers entrusted to it. As more specifically described below, this Complaint concerns a recent targeted ransomware attack and data breach (the "Data Breach") on Fortive's network that resulted in unauthorized access to the highly sensitive data of over 31,000 individuals.

7. Upon information and belief, up to and through November 2023, Defendants obtained Plaintiffs' and Class Members' PII and stored that PII, unencrypted, in an Internet-accessible environment on Defendant Fortive's network, from which unauthorized actors used an extraction tool to retrieve Plaintiffs' and Class Members' sensitive PII.

8. Defendants' network experienced two data breaches that occurred between January 25, 2023, and November 6, 2023. Defendants admit that "in October and November 2023, we detected unusual activity within our network environment stemming from cybersecurity incidents involving **two** separate unauthorized third parties." *See* sample Breach Notice attached as Exhibit A. (emphasis added). The breaches continued for eleven months before Defendants detected them. Following an internal investigation in or around November 2023, Defendants learned cybercriminals had gained unauthorized access to employees' and consumers' PII. *Id.*

9. Upon information and belief, cybercriminals were able to breach Defendants' systems because Defendants failed to adequately train its employees on cybersecurity, failed to adequately monitor its agents, contractors, vendors, and suppliers in handling and securing Plaintiffs' and Class Members' PII, and failed to maintain reasonable security safeguards or protocols to protect Plaintiffs' and Class Members 's PII—rendering them easy targets for cybercriminals.

10. Defendants' cybersecurity was so inadequate that not only did it take it a year and half to recognize that cybercriminals had access to its current and former employees and consumers' most sensitive information, but, following discovery of the Breach in October 2023, Defendants struggled to terminate the cybercriminals' access to their systems until November 6, 2023.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

11. On or about October 3, 2024–over a year and a half after the Data Breach first occurred, Defendants finally began notifying Plaintiffs and Class Members about the Data Breach ("Breach Notice"). *See* Exhibit A.

12. Defendants' Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell employees and consumers how many people were impacted, how the breach happened, or why it took the Defendants over a year and a half to finally begin notifying victims that cybercriminals had gained access to their highly private information.

13. Defendants' failure to timely report the Data Breach made the victims vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

14. Defendants knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

15. In failing to adequately protect its employees' and consumers' PII, adequately notify them about the breach, and obfuscating the nature of the breach, Defendants violated federal and state laws, along with industry standards and harmed thousands of current and former employees and consumers.

16. The harm resulting from a breach of private data manifests in several ways, including identity theft and financial fraud. The exposure of a person's PII through a data breach ensures that such person will be at a substantially increased and certainly impending risk of identity theft crimes compared to the rest of the population, potentially for the rest of their lives. Mitigating that risk—to the extent it is even possible to do so—requires individuals to devote significant time and money to closely monitor their credit, financial accounts, health records, and email accounts, as well as other prophylactic measures.

17. Defendants breached its duty to protect the sensitive PII entrusted to it, failed to abide by its own Privacy Policy, and failed to provide sufficiently prompt notice after learning of the Data Breach. As such, Plaintiffs bring this Class action on behalf of themselves and over 31,000

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

other individuals whose PII was accessed and exposed to unauthorized third parties.

18. As a direct and proximate result of Defendants' inadequate data security, and breach of its duty to handle PII with reasonable care, Plaintiffs' and the Class Members' PII have been accessed by hackers, posted on the dark web, and exposed to an untold number of unauthorized individuals.

19. Plaintiffs are now at a significantly increased and certainly impending risk of fraud, identity theft, misappropriation of health insurance benefits, intrusion of their health privacy, and similar forms of criminal mischief, risk which may last for the rest of their lives. Consequently, Plaintiffs must devote substantially more time, money, and energy to protect themselves, to the extent possible, from these crimes.

20. Plaintiffs, on behalf of themselves and others similarly situated, bring claims for negligence, negligence *per se*, breach of fiduciary duty, breach of confidences, intrusion upon seclusion/invasion of privacy, breach of an implied contract, unjust enrichment, declaratory judgment, violation of California's Unfair Competition Law ("UCL") Cal Bus. & Prof. Code § 17200, *et seq*. and violation of the California Customer Records Act Cal. Civ. Code § 1798.80, *et seq*., seeking actual and putative damages, with attorneys' fees, costs, and expenses, and appropriate injunctive and declaratory relief.

21. To recover from Defendants for their sustained, ongoing, and future harms, Plaintiffs seek damages in an amount to be determined at trial, declaratory judgment, and injunctive relief requiring Defendants to: (1) disclose, expeditiously, the full nature of the Data Breach and the types of PII accessed, obtained, or exposed by the hackers; (2) implement improved data security practices to reasonably guard against future breaches of PII possessed by Defendants; and (3) provide, at its own expense, all impacted victims with lifetime identity theft protection services.

PARTIES

Plaintiff Michael Dudley

22. Plaintiff Michael Dudley is a resident and citizen of Kernersville, North Carolina,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

where he intends to remain. At the time of the Data Breach, Mr. Dudley was a former Fortive employee. Mr. Dudley's PII was stored and handled by Defendants on its systems. On or around October 3, 2024, Defendants notified Mr. Dudley via letter of the Data Breach and the impact to his PII.

Plaintiff Sherry Dudley

23. Plaintiff Sherry Dudley is a resident and citizen of Kernersville, North Carolina, where she intends to remain. At the time of the Data Breach, Ms. Dudley was a former Fortive employee. Ms. Dudley's PII was stored and handled by Defendants on its systems. On or around October 3, 2024, Defendants notified Ms. Dudley via letter of the Data Breach and the impact to her PII. Additionally, she received several alerts from her credit monitoring account stating her social security number and email address were compromised.

Plaintiff Matthew Spaeth

24. Plaintiff Matthew Spaeth is a natural person and citizen of Missouri, where he intends to remain. Plaintiff Spaeth is a former Censis employee and a data breach victim. Plaintiff received a Notice of Data Breach in or around October 2024.

25. As a condition of employment with Censis, Plaintiff provided Defendant with his PII, including at least his name, social security number, driver's license, passport number, birth certificate number, financial account number, credit card number, debit card number, and health insurance information. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

Plaintiff Jennifer Nelson

26. Plaintiff Jennifer Nelson is a natural person and citizen of Minnesota, where she intends to remain. Plaintiff Nelson received Industrial Scientific's Breach Notice on or around October 3, 2024.

Plaintiff Seth Toepfer

27. Plaintiff Seth Toepfer is a natural person and citizen of Texas, where he intends to

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

remain. Plaintiff Toepfer is a former Accruent employee and Data Breach victim.

28. As a condition of employment, Plaintiff Toepfer provided Defendants with his PII, including at least his name, social security number, driver's license, passport number, birth certificate number, financial account number, credit card number, debit card number, and health insurance information. Defendants used that PII to facilitate Plaintiff's employment, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

29. When Plaintiff Toepfer provided his PII to the Defendants, he trusted that the company would use reasonable measures to protect it according to state and federal law.

30. Plaintiff Toepfer received a Notice of Data Breach in or around October 2024.

31. Thus, on information and belief, Plaintiff Toepfer's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff Marilyn Cazares

32. Plaintiff Marilyn Cazares is a natural person and citizen of California, where she intends to remain. Plaintiff Cazares is a former ASPS employee and a data breach victim.

33. As a condition of employment, Plaintiff provided Defendants with her PII, including at least her name, social security number, date of birth, driver's license, passport number, birth certificate number, financial account number, credit card number, debit card number, and health insurance information. Defendants used that PII to facilitate Plaintiff's employment, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

34. Plaintiff Cazares provided her PII to Defendants and trusted that the company would use reasonable measures to protect it according to state and federal law.

35. Plaintiff Cazares received a Notice of Data Breach in or around October 2024.

36. Thus, on information and belief, Plaintiff Cazares' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

37. As a result of Defendants' conduct, Plaintiffs suffered actual damages including,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

without limitation, time related to monitoring their financial accounts for fraudulent activity, facing an increased and imminent risk of fraud and identity theft, the lost value of their personal information, and other economic and non-economic harm. Plaintiffs and Class Members will now be forced to expend additional time, efforts, and potentially expenses to review their credit reports, monitor their financial accounts, and monitor for fraud or identify theft – particularly since the compromised information may include Social Security numbers.

Defendant Fortive Corporation

38. Defendant Fortive Corporation ("Fortive") is a provider of services with its headquarters at 6920 Seaway Boulevard in Everett, Washington. Defendant Fortive Corp. is a Delaware corporation registered in good standing in Washington.

39. Fortive is an affiliate or parent company of numerous other companies, including but not limited to Accruent, Advanced Sterilization Products, Anderson Instrument Co., Censis Technologies, Dover Motion, Dynapar Corporation, Fluke Biomedical, Fluke Corp., FTV Employment Services, Global Physics Solutions, Industrial Scientific Corporation, Intelex Technologies US, Janos Technology, Pacific Scientific Energetic Materials Company, Provation Software, Qualitrol Company, ServiceChannel.com, Inc., Setra Systems, Tektronix, Inc., The Gordian Group, each of which was subjected to the data breach.

40. Defendant, Accruent, is a limited liability company registered in Delaware, with its principal place of business located at 11500 Alterra Parkway Suite 110 Austin, Texas 78758.

41. Accruent touts itself to be "the world's leading provider of workplace and asset management software for unifying the built environment."[4] It boasts an annual revenue of $270 million.[5]

42. Defendant, Advanced Sterilization Products Services Inc., is a New Jersey corporation, with its principal place of business located at 33 Technology Drive, Irvine, California

[4] Accruent, https://www.accruent.com/about-us (last visited October 14, 2024).
[5] Zoominfo, Accruent, https://www.zippia.com/accruent-careers-13439/revenue/ (last visited October 14 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

92618. ASP is a Fortive operating company.

43. ASPS touts itself to be "a leader in infection prevention, dedicated to creating the products, solutions, and processes needed by practitioners to protect patients during their most critical moments."[6] It boasts an annual revenue of $426.2 million.[7]

44. Defendant, Advanced Sterilization Products Inc, is a Delaware corporation with its principal place of business located at 33 Technology Drive Irvine, California 92618.

45. Defendant Censis is an incorporated company with its principal place of business located in 4031 Aspen Grove Drive, Suite 350, Franklin TN 37067-2950. Censis touts itself to be "an industry leader in surgical instrument management systems, offering advanced web-based software systems." [8] It boasts an annual revenue of $28.6 million.[9]

46. On information and belief, Censis accumulates highly private PII of its current and former employees.

47. In collecting and maintaining its employees' PII, Defendant agreed it would safeguard the data in accordance with state law and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

48. Censis understood the need to protect its current and former employees' PII and prioritize its data security.

49. Defendant Industrial Scientific is a Pennsylvania corporation, with its principal place of business at 1 Life Way Pittsburgh, Pennsylvania 15205. Industrial Scientific is a "leader in lifesaving products and technologies that improve in-the-moment safety outcomes for workers

[6] ASPS, https://www.asp.com/en-us/about (last visited October 24, 2024).
[7] Zoominfo, ASPS, https://www.zoominfo.com/c/advanced-sterilization-products-inc/590548 (last visited October 24, 2024).
[8] Censis, https://censis.com/ (last visited October 8, 2024).
[9] Zoominfo, https://www.zoominfo.com/c/censis-technologies-inc/22827725 (last visited October 8, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

worldwide."[10] Industrial Scientific boasts a total annual revenue of over $169.8 million.[11]

50. Industrial Scientific's services are specialized for clients who oversee highly sensitive data. Industrial Scientific thus must oversee, manage, and protect the PII of its clients' customers, Industrial Scientific's consumers.

51. On information and belief, third-party consumers, whose PII Industrial Scientific collected, do not directly do any business with Industrial Scientific.

52. As a self-proclaimed leader in its industry handling highly sensitive aspects of its clients' business, Industrial Scientific understood the need to protect its client's customers' data and prioritize its data security.

JURISDICTION AND VENUE

53. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332(d). The amount in controversy in this Class action exceeds $5,000,000, exclusive of interest and costs, and there are numerous Class members who are citizens of states other than Defendants' states of citizenship.

54. This Court has personal jurisdiction over Defendants in this case because Defendant Fortive, the parent company for all other Defendants, is headquartered and has its principal place of business in this District and all Defendants conduct substantial business and have minimum contacts with the State of Washington.

55. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant Fortive is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL BACKGROUND

Defendants and the Services Provided.

56. Defendant Fortive is a technology conglomerate established in the United States

[10] Industrial Scientific, About us, https://www.indsci.com/en/about (last visited October 11, 2024).

[11] Industrial Scientific Revenue, Zippia https://www.zippia.com/industrial-scientific-careers-588123/revenue/ (last visited October 11, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

with global operations and sales. Established in 2016, as a spin-off from Danaher Corp., the Defendants have over 18,000 employees with facilities in over 60 countries. Its global revenue in 2023 exceeded $6 billion.[12]

57. On information and belief, Fortive maintains employees' and consumers' PII, including but not limited to:

a. name, residential address, phone number and email address

b. date of birth

c. demographic information

d. Social Security number

e. tax identification number

f. financial information

g. medication information

h. health insurance information

i. photo identification

j. employment information, and

k. other information that Defendants may deem necessary to provide its services.

58. Plaintiffs and Class Members directly or indirectly entrusted Defendants with sensitive and confidential PII, which includes information that is static, does not change, and can be used to commit myriad financial and other crimes.

59. By obtaining, collecting, and storing Plaintiffs' and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known that Defendants were responsible for protecting Plaintiffs' and Class Members' PII from unauthorized disclosure.

60. Plaintiffs and the Class Members relied on Defendants to implement and follow adequate data security policies and protocols, to keep their PII confidential and securely

[12] *See* Fortive Corporation Form 10-K, February 27, 2024, https://investors.fortive.com/sec-filings/all-sec-filings/content/0001659166-24-000046/ftv-20231231.htm (last visited October 10, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

maintained, to use such PII solely for business purposes, and to prevent the unauthorized disclosures of the PII.

61. If Plaintiffs and Class Members had known that Defendants would not take reasonable and appropriate steps to protect their sensitive and valuable PII, they would not have entrusted it to Defendants.

Defendants Knew the Risks of Storing Valuable PII and the Foreseeable Harm to its Employees and Consumers.

62. At all relevant times, Defendants knew it was storing sensitive PII and that, as a result, its systems would be an attractive target for cybercriminals.

63. Defendants also knew that a breach of its systems, and exposure of the information stored therein, would result in the increased risk of identity theft and fraud against the 31,000 individuals whose PII was compromised.

64. These risks are not theoretical. The financial industry has become a prime target for threat actors.

65. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack.

66. In tandem with the increase in data breaches, the rate of identity theft complaints has also increased over the past few years. For instance, in 2017, 2.9 million people reported some form of identity fraud compared to 5.7 million people in 2021.[13]

67. The type and breadth of data compromised in the Data Breach makes the information particularly valuable to thieves and leaves Defendants' employees and consumers especially vulnerable to identity theft, tax fraud, medical fraud, credit and bank fraud, and more.

[13] *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance Information Institute, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20 (last visited Apr. 17, 2023).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

68. PII is a valuable property right.[14] The value of PII as a commodity is measurable.[15] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[16] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in 2018.[17] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

69. As a result of their real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and become more valuable to thieves and more damaging to victims.

70. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches: "[I]n 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 has been sold or posted on the [Dark] Web, fraudulent use of that information may continue for years. As a result, studies that attempt to

---

[14] *See* Marc Van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION & COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible …").

[15] Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle. /824192.

[16] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en.

[17] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

measure the harm resulting from data breaches cannot necessarily rule out all future harm."[18]

71. Even if stolen PII does not include financial or payment card account information, that does not mean there has been no harm, or that the breach does not cause a substantial risk of identity theft. Freshly stolen information can be used with success against victims in specifically targeted efforts to commit identity theft known as social engineering or spear phishing. In these forms of attack, the criminal uses the previously obtained PII about the individual, such as name, address, email address, and affiliations, to gain trust and increase the likelihood that a victim will be deceived into providing the criminal with additional information.

72. Consumers place a high value on the privacy of that data. Researchers shed light on how much consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[19]

73. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

74. Based on the value of its consumers' PII to cybercriminals and the growing rate of data breaches, Defendants certainly knew the foreseeable risk of failing to implement adequate cybersecurity measures.

1. ***Defendants Breached its Duty to Protect its Employees' and Consumers' PII.***

75. On or around October 3, 2024, Defendant Fortive first provided notice of the data breach:

> In October and November 2023, we detected unusual activity within our network environment stemming from cybersecurity incidents involving two separate unauthorized third parties. Upon becoming aware of this issue, we immediately

[18] United States Government Accountability Office, Report to Congressional Requesters, Personal Information, June 2007: https://www.gao.gov/new.items/d07737.pdf (last visited Apr. 17, 2023).

[19] Janice Y. Tsai *et al*., *The Effect of Online Privacy Information on Purchasing Behavior*, *An Experimental Study*, 22(2) Information Systems Research 254 (June 2011), https://www.guanotronic.com/~serge/papers/weis07.pdf.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

> engaged leading external cybersecurity experts to assist us in thoroughly investigating the incidents. The investigation identified that the unauthorized third parties gained access to our network and viewed and acquired data between January 25, 2023 and November 6, 2023, at which point their access was terminated.
>
> Based on our investigation and comprehensive review of potentially affected data, which concluded on September 3, 2024, we can confirm that certain personal information was involved in the incidents, and that your personal information was affected. Once our comprehensive investigation was concluded, we worked to notify you as quickly as we could. [20]

76. To date, Defendants investigation has determined that the private information of roughly 31,000 current and former employees, customers and other affiliated individuals was accessed and compromised by unauthorized users on two separate occasions between January 25, 2023, and November 6, 2023.

77. Fortive, along with at least 20 of its subsidiaries, including but not limited to Accruent and ASPS, had their most sensitive information accessed and stolen during this Breach. The Fortive subsidiaries impacted by the Breach are listed below:

a. Accruent: at least 2, 513 individuals impacted;

b. Advanced Sterilization Products: at least 3,513 individuals impacted;

c. Censis Technologies: at least 296 individuals impacted;

d. Fluke Corporation: at least 6,661 individuals impacted;

e. Industrial Scientific Corporation: at least 1,459 individuals impacted;

f. Pacific Scientific Energetic Materials Company: at least 2,070 individuals impacted;

g. Setra Systems: at least 1,919 individuals impacted;

h. The Gordian Group: at least 1,489 individuals impacted;

i. FTV Employment Services: at least 10,680 individuals impacted;

j. Dover Motion: at least 575 individuals impacted;

k. Anderson Instrument Co.: number of individuals impacted currently unknown;

[20] See Maine Consumer Protection Bureau Notice, ftv-employment-20241003, mm.nh.gov (last visited October 10, 2024.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

l. Dynapar Corporation: number of individuals impacted currently unknown;

m. Fluke Biomedical: number of individuals impacted currently unknown;

n. Global Physics Solutions: number of individuals impacted currently unknown;

o. Intelex Technologies US: number of individuals impacted currently unknown;

p. Provation Software: number of individuals impacted currently unknown;

q. Qualitrol Company: number of individuals impacted currently unknown;

r. ServiceChannel.com Inc.: number of individuals impacted currently unknown;

s. Tektronix In.: number of individuals impacted currently unknown;

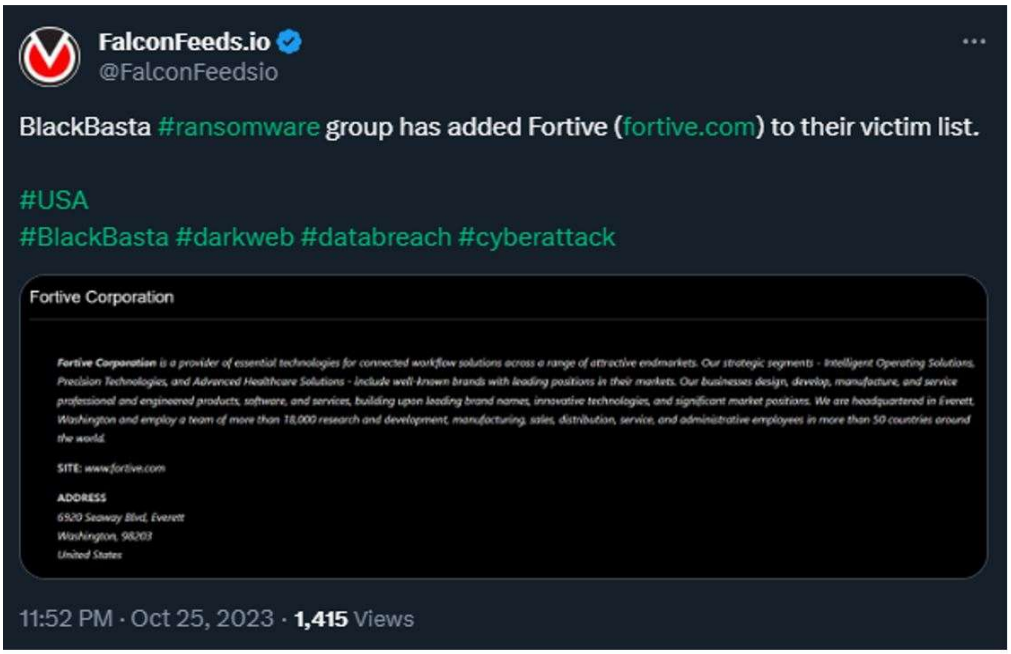
t. Janos Technology: number of individuals impacted currently unknown.

78. Through their inadequate security practices, Defendants exposed Plaintiffs' and the Class Members' PII for theft and sale on the dark web.

79. On information and belief, the notorious Black Basta ransomware gang was one of the cybercriminals responsible for the cyberattack. Black Basta is one of the most active hackers, having hacked over 50 companies around the world within mere months, Black Basta frequently posts the stolen private information for sale.[21] Defendants knew or should have known of the tactics that hackers like Black Basta employ.

[21] Black Basta Ransomware, Tripwire,https://www.tripwire.com/state-of-security/black-basta-ransomware-what-you-need-to-know (last visited June 3, 2023).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com



80. It is likely the Data Breach was targeted at Defendants due to its status as an information and technological services provider that collects, creates, and maintains sensitive PII.

81. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data of specific individuals, including (among other things) Plaintiffs' and Class Members' PII.

82. With the PII secured and stolen by Black Basta, the hackers then purportedly issued a ransom demand to Defendants. However, Defendants have provided no public information on the ransom demand or payment.

83. On information and belief, Black Basta plans to release all stolen information obtained from the data breach onto its leak page.

84. While Defendants' Notice stated that it would directly notify the affected individuals and that it is committed to keeping the victims informed, upon information and belief Defendants have failed to directly notify numerous Class Members.

85. Upon information and belief, and based on the type of cyberattack, it is plausible and likely that Plaintiffs' PII was stolen in the Data Breach. Plaintiffs further believe their PII was

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

likely subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals.

86. Defendants had a duty to adopt appropriate measures to protect Plaintiffs' and Class Members' PII from involuntary disclosure to third parties.

87. In response to the Data Breach, Defendant Fortive admits it worked with external "security experts" to determine the nature and scope of the incident and claims to have taken steps to secure the systems. Defendant Fortive admits additional security was required, but there is no indication whether these steps will be adequate to protect Plaintiffs' and Class Members' PII going forward.

88. Because of the Data Breach, data thieves were able to gain access to Defendants' private systems beginning in January 2023 and continuing to November 2023, and were able to compromise, access, and acquire Plaintiffs' and Class Members protected PII.

89. Fortive had obligations created by contract, industry standards, common law, and its own promises and representations made to Plaintiffs and Class Members to keep their PII confidential and to protect them from unauthorized access and disclosure.

90. Plaintiffs and the Class Members reasonably relied (directly or indirectly) on Defendants' sophistication to keep their sensitive PII confidential; to maintain proper system security; to use this information for business purposes only; and to make only authorized disclosures of their PII.

91. Plaintiffs' and Class Members unencrypted, unredacted PII was compromised due to Defendants' negligent and/or careless acts and omissions, and due to the utter failure to protect Class Members' PII. Criminal hackers obtained their PII because of its value in exploiting and stealing Plaintiffs and Class Members identities. The heightened risks to Plaintiffs and Class Members will remain for their respective lifetimes.

FTC Guidelines Prohibit Defendants from Engaging in Unfair or Deceptive Acts or Practices.

92. Defendants are prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTC Act") from engaging in "unfair or deceptive acts or practices in or affecting commerce."

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act.

93. The FTC has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[22]

94. The FTC provided cybersecurity guidelines for businesses, advising that businesses should protect personal customer information, properly dispose of personal information that is no longer needed, encrypt information stored on networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[23]

95. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private data; require complex passwords to be used on networks; use industry-tested methods for security; monitor suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.[24]

96. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

97. Defendants failed to properly implement basic data security practices. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to

---

[22] *Start with Security – A Guide for Business*, United States Federal Trade Comm'n (2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[23] *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm'n, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

[24] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

consumers' PII constitutes an unfair act of practice prohibited by Section 5 of the FTC Act.

Cyberattacks and Data Breaches Cause Disruption and Put Consumers at an Increased Risk of Fraud and Identity Theft.

98. Cyberattacks and data breaches at companies like Defendants are especially problematic because they can negatively impact on the daily lives of individuals affected by the attack.

99. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[25]

100. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, and to take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

101. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to exhaust financial accounts, receive medical treatment, open new utility accounts, and incur charges

[25] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

and credit in a person's name.

102. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing freezes on their credit, and correcting their credit reports.[26]

103. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. According to Experian, one of the largest credit reporting companies in the world, "[t]he research shows that personal information is valuable to identity thieves, and if they can get access to it, they will use it" to among other things: open a new credit card or loan, change a billing address so the victim no longer receives bills, open new utilities, obtain a mobile phone, open a bank account and write bad checks, use a debit card number to withdraw funds, obtain a new driver's license or ID, and/or use the victim's information in the event of arrest or court action.

104. Identity thieves can also use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, and/or rent a house or receive medical services in the victim's name.

105. Moreover, theft of PII is also gravely serious because PII is an extremely valuable property right.[27]

106. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States. For example, with the PII stolen in the Data Breach, which includes Social Security

---

[26] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last accessed Feb. 24, 2023).

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

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

numbers, identity thieves can open financial accounts, commit medical fraud, apply for credit, file fraudulent tax returns, commit crimes, create false driver's licenses and other forms of identification and sell them to other criminals or undocumented immigrants, steal government benefits, give breach victims' names to police during arrests, and many other harmful forms of identity theft. These criminal activities have and will result in devastating financial and personal losses to Plaintiffs and Class members.

107. As discussed above, PII is such a valuable commodity to identity thieves, and once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

108. Social security numbers are particularly sensitive pieces of personal information. As the Consumer Federation of America explains:

> **Social Security number:** *This is the most dangerous type of personal information in the hands of identity thieves* because it can open the gate to serious fraud, from obtaining credit in your name to impersonating you to get medical services, government benefits, your tax refund, employment—even using your identity in bankruptcy and other legal matters. It's hard to change your Social Security number and it's not a good idea because it is connected to your lift in so many ways. [28]

109. For instance, with a stolen Social Security number, which is only one subset of the PII compromised in the Data Breach, someone can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[29]

110. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[30] Such fraud may go undetected until debt collection calls commence months, or even years later. Stolen Social Security

---

[28] *See, e.g.*, Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number* (Nov. 2, 2017), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/ (emphasis added).

[29] *Id.*

[30] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[31] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected because one was already filed on their behalf.

111. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[32]

112. This was a financially motivated Data Breach, as the only reason the cybercriminals go through the trouble of running a targeted cyberattack against companies like Fortive is to get information that they can monetize by selling on the black market for use in the kinds of criminal activity described herein. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."

113. Indeed, a Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[33] "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[34]

---

[31] *Id.* at 4.

[32] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft.

[33] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[34] *Dark Web Monitoring: What You Should Know*, Consumer Federation of America (Mar. 19,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

114. These risks are both certainly impending and substantial. As the FTC has reported, if hackers get access to PII, they *will use it.*[35]

115. There may also be a time lag between when sensitive personal information is stolen, when it is used, and when a person discovers it has been used. Fraud and identity theft resulting from the Data Breach may go undetected until debt collection calls commence months, or even years, later. As with income tax returns, an individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud.

116. For example, on average it takes approximately three months for consumers to discover their identity has been stolen and used, and it takes some individuals up to three years to learn that information.[36]

117. Cybercriminals can post stolen PII on the cyber black market for years following a data breach, thereby making such information publicly available.

118. Approximately 21% of victims did not realize their identity has been compromised until more than two years after it happened. [37] This gives thieves ample time to seek multiple treatments under the victim's name.

119. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[38]

120. It is within this context that Plaintiffs must now live with the knowledge that their PII is forever in cyberspace and was taken by people willing to use the information for any number

---

2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

[35] *Id.*

[36] John W. Coffey, *Difficulties in Determining Data Breach Impacts*, 17 JOURNAL OF SYSTEMICS, CYBERNETICS AND INFORMATICS 9 (2019), http://www.iiisci.org/journal/pdv/sci/pdfs/IP069LL19.pdf.

[37] *See* Medical ID Theft Checklist, https://www.identityforce.com/blog/medical-id-theft-checklist-2 (last visited Apr. 17, 2023).

[38] *Guide for Assisting Identity Theft Victims*, FED. TRADE COMM'N, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

of improper purposes and scams, including making the information available for sale on the black market.

121. Victims of the Data Breach, like Plaintiffs, must spend many hours and large amounts of money protecting themselves from the current and future negative impacts to their privacy and credit because of the Data Breach.[39]

122. As a direct and proximate result of the Data Breach, Plaintiffs have had their PII exposed, have suffered harm and have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft. Plaintiffs must now take the time and effort (and spend the money) to mitigate the actual and potential impact of the Data Breach on their everyday lives, including purchasing identity theft and credit monitoring services every year for the rest of their lives, placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions and healthcare providers, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and health insurance account information for unauthorized activity for years to come.

123. Moreover, Plaintiffs and Class Members have an interest in ensuring that their PII, which remains in Defendants' possession, is protected from further public disclosure by the implementation of better employee training and industry standard and statutorily compliant security measures and safeguards. Defendants have shown themselves to be wholly incapable of protecting Plaintiffs' PII.

124. Plaintiffs and Class Members also have an interest in ensuring that their personal information that was provided to Defendants is removed from Defendants' unencrypted files.

125. Because of the value of its collected and stored data, Defendants knew or should have known about these dangers and strengthened their data security accordingly. Defendants were put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

---

[39] *Id.*

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

126. Defendants received Plaintiffs' and Class Members' PII in connection with providing certain services for them. In requesting and maintaining Plaintiffs' PII for business purposes, Defendants expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiffs' and Class Members' PII. Defendants did not, however, take proper care of Plaintiffs' and Class Members' PII, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendants' inadequate security measures.

Plaintiffs Michael Dudley and Sherry Dudley's Experience and Injuries

127. Plaintiff Sherry Dudley is a former employee of Gilbarco Veeder-Root which during her time of employment was a subsidiary of Defendant Fortive.

128. Plaintiff Michael Dudley is a current employee of Gilbarco Veeder-Root and was an employee there while it was still owned by Defendant Fortive.

129. Beginning in approximately December 2023 and January 2024, Plaintiffs Sherry and Michael Dudley noticed a significant increase in spam calls, texts and emails.

130. Additionally, Ms. Dudley received several alerts from her credit monitoring account stating her social security number and email address were compromised.

131. Plaintiffs Sherry and Michael Dudley have received notifications from Creditwise that their PII is on the dark web.

132. Due to the Defendants' delay in notifying them of the Data Breach, Defendants deprived the Dudley Plaintiffs of the earliest opportunity to guard themselves against the Data Breach's effects.

133. As a result of Defendants' inadequate cybersecurity, Defendants exposed the Dudley Plaintiffs' PII to theft by cybercriminals and sale on the dark web.

134. The Dudley Plaintiffs suffered actual injury from the exposure of their PII —which violates their rights to privacy.

135. The Dudley Plaintiffs suffered actual injury in the form of damage to and diminution in the value of their PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

136. As a result of the Data Breach, The Dudley Plaintiffs have spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing their online account passwords, placing a credit freeze on all the three main credit bureaus, and monitoring their credit information.

137. The Dudley Plaintiffs have already spent and will continue to spend considerable time and effort monitoring their accounts to protect themselves from identity theft. The Dudley Plaintiffs fear for their personal financial security and uncertainty over what PII was exposed to in the Data Breach. The Dudley Plaintiffs have and are now experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

138. The Dudley Plaintiffs are now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from their PII being placed in the hands of unauthorized third parties. This injury was worsened by the Defendants' failure to inform the Dudley Plaintiffs about the Data Breach in a timely fashion.

Plaintiff Matthew Spaeth's Experience and Injuries

139. Plaintiff Spaeth provided his PII to Defendant Censis and trusted that the company would use reasonable measures to protect it according to state and federal law.

140. Plaintiff Spaeth received a Notice of Data Breach in or around October 2024.

141. Thus, on information and belief, Plaintiff Spaeth's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

142. Defendant deprived Plaintiff Spaeth of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about the Breach for a year.

143. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Spaeth's PII for theft by cybercriminals and sale on the dark web.

144. Plaintiff Spaeth suffered actual injury from the exposure of his PII —which violates

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

his rights to privacy.

145. Plaintiff Spaeth suffered actual injury in the form of damage to and diminution in the value of his PII. After all, PII is a form of intangible property that Defendant was required to adequately protect.

146. As a result of the Data Breach, Plaintiff Spaeth has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through all the three main credit bureaus, and monitoring Plaintiff Spaeth's credit information.

147. Plaintiff Spaeth has already spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Spaeth fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Spaeth has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. Plaintiff Spaeth is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of his Social Security number, will impact his ability to do so. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

148. Plaintiff Spaeth is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff Spaeth about the Data Breach in a timely fashion.

149. Indeed, shortly after the Data Breach, Plaintiff Spaeth began suffering a significant increase in spam calls, forcing him to turn phone to not accept calls from unknown numbers. These spam calls suggest that his PII is now in the hands of cybercriminals.

150. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

and steal even more information.[40] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

151. Plaintiff Spaeth has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Jennifer Nelson's Experience and Injuries

152. As a result of Defendants' inadequate cybersecurity, Defendant deprived Plaintiff Nelson of the earliest opportunity to guard herself against the Data Breach's effects by failing to properly notify her.

153. As a further result, Defendant exposed Plaintiff Nelson's PII for theft by numerous cybercriminals and sale on the dark web.

154. Plaintiff Nelson does not recall ever learning that her PII was compromised in a data breach incident, other than the breach at issue in this case.

155. As a result of the Data Breach notice, Plaintiff Nelson spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

156. Plaintiff Nelson has and will spend considerable time and effort monitoring her accounts to protect herself from additional identity theft. Plaintiff Nelson fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

157. Plaintiff Nelson has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

158. Plaintiff Nelson suffered actual injury in the form of damages to and diminution in

[40] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

the value of Plaintiff Nelson's PII—a form of intangible property that Plaintiff Nelson entrusted to Defendant, which was compromised in and as a result of the Data Breach.

159. Plaintiff Nelson suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

160. Plaintiff Nelson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties and possibly criminals.

161. Indeed, shortly after the Data Breach, Plaintiff Nelson began suffering a significant increase in spam calls, forcing him to turn phone to not accept calls from unknown numbers. These spam calls suggest that her PII is now in the hands of cybercriminals.

162. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[41] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

163. Plaintiff Nelson has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Seth Toepfer's Experience and Injuries

164. Plaintiff Toepfer is a former Accruent employee and a data breach victim.

165. Due to the Defendants' delay in notifying him of the Data Breach, Defendants deprived Plaintiff Toepfer of the earliest opportunity to guard himself against the Data Breach's effects.

166. As a result of Defendants' inadequate cybersecurity, Defendants exposed Plaintiff Toepfer's PII to theft by cybercriminals and sale on the dark web.

167. Plaintiff Toepfer suffered actual injury from the exposure of his PII —which

[41] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

violates his rights to privacy.

168. Plaintiff Toepfer suffered actual injury in the form of damage to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

169. As a result of the Data Breach, Plaintiff Toepfer has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze on all the three main credit bureaus, and monitoring Plaintiff's credit information.

170. Plaintiff Toepfer has already spent and will continue to spend considerable time and effort monitoring his accounts to protect himself from identity theft. Plaintiff Toepfer fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach. Plaintiff Toepfer has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. Plaintiff Toepfer is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of his Social Security number, will impact his ability to do so. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

171. Plaintiff Toepfer is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties. This injury was worsened by the Defendants' failure to inform Plaintiff Toepfer about the Data Breach in a timely fashion.

172. Indeed, shortly after the Data Breach, Plaintiff Toepfer began suffering a significant increase in spam calls. These spam calls suggest that his PII is now in the hands of cybercriminals.

173. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

and steal even more information.[42] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

174. Plaintiff Toepfer has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected, and safeguarded from future breaches.

Plaintiff Marilyn Cazares's Experience and Injuries

175. Defendants deprived Plaintiff Cazares of the earliest opportunity to guard herself against the Data Breach's effects by failing to notify her about the Breach for a year.

176. As a result of their inadequate cybersecurity, Defendants exposed Plaintiff Cazares' PII to theft by cybercriminals and sale on the dark web.

177. Plaintiff Cazares suffered actual injury from the exposure of her PII —which violates her rights to privacy.

178. Plaintiff Cazares suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendants were required to adequately protect.

179. Plaintiff Cazares does not recall ever learning that her PII was compromised in a data breach incident, other than the breach at issue in this case.

180. As a result of the Data Breach, Plaintiff Cazares has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing her online account passwords, placing a credit freeze through all the three main credit bureaus, and monitoring Plaintiff Cazares credit information.

181. Plaintiff Cazares has already spent and will continue to spend considerable time and effort monitoring her accounts to protect herself from identity theft. Plaintiff Cazares fears for her personal financial security and uncertainty over what PII was exposed in the Data Breach.

[42] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Plaintiff Cazares has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. Plaintiff Cazares is experiencing anxiety, distress, and fear regarding how this Data Breach, including the exposure and loss of her Social Security number, will impact her ability to do so. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

182. Plaintiff Cazares is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from her PII being placed in the hands of unauthorized third parties. This injury was worsened by the Defendants' failure to inform Plaintiff about the Data Breach in a timely fashion.

183. Indeed, shortly after the Data Breach, Plaintiff Cazares began suffering a significant increase in spam calls and voicemail relating to fraudulent loans. These spam calls suggest that her PII is now in the hands of cybercriminals.

184. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[43] On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach.

185. Plaintiff Cazares has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiffs Suffered Damages.

186. Once an individual's PII is for sale and access on the dark web, as Plaintiffs' PII is here because of the Breach, cybercriminals can use the stolen and compromised to gather and steal even more information.

187. For the reasons mentioned above, the Defendants' conduct, which allowed the Data

[43] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited January 9, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Breach to occur, caused Plaintiffs and Class Members significant injuries and harm in several ways. Plaintiffs and Class Members must immediately devote time, energy, and money to: (1) closely monitor their medical statements, bills, records, and credit and financial accounts; (2) change login and password information on any sensitive account even more frequently than they already do; (3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and (4) search for suitable identity theft protection and credit monitoring services, and pay to procure them. Plaintiffs and Class Members have taken or will be forced to take these measures in order to mitigate their potential damages as a result of the Data Breach.

188. Once PII is exposed, there is little that can be done to ensure that the exposed information has been fully recovered or obtained against future misuse. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives because of Defendants' conduct.

189. Further, the value of Plaintiffs and Class Members' PII has been diminished by its exposure in the Data Breach. Plaintiffs and Class Members did not receive the full benefit of their bargain when paying for services, and instead received services that were of a diminished value to those described in their agreements with Defendants for the benefit and protection of Plaintiffs and their respective PII. Plaintiffs and Class Members were damaged in an amount at least equal to the difference in the value between the services they thought they paid for (which would have included adequate data security protection) and the services they received.

190. Plaintiffs and Class Members would not have obtained services or employment from Defendants or worked for or paid the amount they did to receive such services, had they known that Defendants would negligently fail to protect their PII. Indeed, Plaintiffs and Class Members worked for or paid for services with the expectation that Defendants would keep their PII secure and inaccessible from unauthorized parties. Plaintiffs and Class Members would not have obtained services from Defendants had they known that Defendants failed to properly train its employees, lacked safety controls over its computer network, and did not have proper data

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

security practices to safeguard their PII from criminal theft and misuse.

191. As a result of Defendants' failures, Plaintiffs and Class Members are also at substantial and certainly impending increased risk of suffering identity theft and fraud or other misuse of their PII.

192. Further, because Defendants delayed posting a notice of the Data Breach on its website for over a year and a half and delayed sending mail notice of the same to Plaintiffs and Class Members, Plaintiffs and Class members were unable to take affirmative steps during that time period to attempt to mitigate any harm or take prophylactic steps to protect against injury.

193. From a recent study, 28% of consumers affected by a data breach become victims of identity fraud—this is a significant increase from a 2012 study that found only 9.5% of those affected by a breach would be subject to identity fraud. Without a data breach, the likelihood of identify fraud is only about 3%.[44]

194. Plaintiffs are also at a continued risk because their information remains in Defendants' computer systems, which have already been shown to be susceptible to compromise and attack and is subject to further attack so long as Defendants fails to undertake the necessary and appropriate security and training measures to protect their employees' and consumers' PII.

195. In addition, Plaintiffs and Class Members have suffered emotional distress because of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized exposure of their private information to strangers.

CLASS ALLEGATIONS

196. Plaintiffs bring all counts, as set forth below, individually and as a Class action, pursuant to the provisions of the Fed. R. Civ. P. 23, on behalf of a Class defined as:

> All persons in the United States who had their Private Information submitted to Defendants or Defendants' affiliates and/or whose Private Information was compromised because of the data breach(es) by Defendants, including all those who received a Notice of the Data Breach (the "Class").

[44] Stu Sjouwerman, *28 Percent of Data Breaches Lead to Fraud*, KNOWBE4, https://blog.knowbe4.com/bid/252486/28-percent-of-data-breaches-lead-to-fraud (last visited Feb. 29, 2024).

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

197. Plaintiff Marilyn Cazares seeks certification of a California Subclass as defined below:

> California Subclass: All individuals residing in California whose PII was submitted to Defendants or Defendants' affiliates and/or whose PII was compromised because of the data breach(es) by Defendants, including all those who received a Notice of the Data Breach (the "California Subclass").

198. Excluded from the Class are Defendants, their subsidiaries and affiliates, officers and directors, any entity in which Defendants have a controlling interest, the legal representative, heirs, successors, or assigns of any such excluded party, the judicial officer(s) to whom this action is assigned, and the members of their immediate families.

199. This proposed Class definition is based on the information available to Plaintiffs currently. Plaintiffs may modify the Class definition in an amended pleading or when they move for Class certification, as necessary to account for any newly learned or changed facts as the situation develops and discovery gets underway.

200. **Numerosity – Fed. R. Civ. P. 23(a)(1)**: Plaintiffs are informed and believe, and thereon allege, that there are at minimum, tens of thousands of members of the Class described above. The exact size of the Class and the identities of the individual members are identifiable through Defendants' records, including but not limited to the files implicated in the Data Breach, but based on public information, the Class includes more than 31,000 individuals.

201. **Commonality – Fed. R. Civ. P. 23(a)(2):** This action involves questions of law and fact common to the Class. Such common questions include, but are not limited to:

a. Whether Defendants failed to timely notify Plaintiffs and Class Members of the Data Breach;

b. Whether Defendants have a duty to protect Plaintiffs' and Class Members' PII;

c. Whether Defendants were negligent in collecting and storing Plaintiffs and Class Members' PII, and breached their duties thereby;

d. Whether Defendants breached their fiduciary duty to Plaintiffs and the Class;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

e. Whether Defendants breached their duty of confidence to Plaintiffs and the Class;

f. Whether Defendants violated their own Privacy Practices;

g. Whether Defendants entered a contract implied in fact with Plaintiffs and the Class;

h. Whether Defendants breached that contract by failing to adequately safeguard Plaintiffs and Class members' PII;

i. Whether Defendants were unjustly enriched;

j. Whether Plaintiffs and Class Members are entitled to damages as a result of Defendants' wrongful conduct; and

k. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendants' wrongful conduct.

202. **Typicality – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs' claims are typical of the claims of the members of the Class. The claims of the Plaintiffs and members of the Class are based on the same legal theories and arise from the same unlawful and willful conduct. Plaintiffs and members of the Class all had information stored in Defendants' system, each having their PII exposed and/or accessed by an unauthorized third party.

203. **Adequacy of Representation – Fed. R. Civ. P. 23(a)(3)**: Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the other Class Members Plaintiffs seek to represent; Plaintiffs have retained counsel competent and experienced in complex Class action litigation; Plaintiffs intend to prosecute this action vigorously; and Plaintiffs' counsel have adequate financial means to vigorously pursue this action and ensure the interests of the Class will not be harmed. Furthermore, the interests of the Class members will be fairly and adequately protected and represented by Plaintiffs and Plaintiffs' counsel.

204. **Injunctive Relief, Fed. R. Civ. P. 23(b)(2):** Defendants have acted and/or refused to act on grounds that apply generally to the Class therefore making injunctive and/or declarative

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

relief appropriate with respect to the Class under 23(b)(2).

205. **Superiority, Fed. R. Civ. P. 23(b)(3):** A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, the conduct of this action as a Class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

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

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

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

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

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

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

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

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

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

208. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Defendants have already preliminarily identified Class Members for the purpose of sending notice of the Data Breach.

FIRST CAUSE OF ACTION
NEGLIGENCE
(Plaintiffs on behalf of the Class)

209. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

210. Plaintiffs bring this claim individually and on behalf of the Class.

211. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, and control.

212. Defendants' duty to use reasonable care arose from several sources, including but not limited to those described below.

213. Defendants have a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices on the part of the Defendants. By collecting and storing valuable PII that is routinely targeted by criminals for unauthorized access, Defendants were obligated to act with reasonable care to protect against these foreseeable threats.

214. Defendants' duty also arose from the fact that it holds itself out as a trusted provider of technology services, and thereby assumes a duty to reasonably protect consumers' information.

215. Defendants breached the duties owed to Plaintiffs and Class Members and thus were negligent. As a result of a successful attack directed towards Defendants that compromised Plaintiffs and Class Members' PII, Defendants breached their duties through some combination of

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

the following errors and omissions that allowed the data compromise to occur:

a. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

b. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

c. failing to design and implement information safeguards to control these risks;

d. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

e. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

f. failing to detect the breach at the time it began or within a reasonable time thereafter;

g. failing to follow its own privacy policies and practices published to its employees and consumers; and

h. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

216. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

217. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered injuries, including, but not limited to:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

218. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(Plaintiffs on behalf of the Class)

219. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

220. Plaintiffs bring this claim individually and on behalf of the Class.

221. Section 5 of the FTC Act prohibits "unfair … practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by entities such as Defendants for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendants' duty.

222. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with the industry standards. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of a data breach involving PII of its employees and consumers.

223. Plaintiffs and Class Members are consumers within the Class of persons Section 5 of the FTC Act was intended to protect.

224. The defendants' violation of Section 5 of the FTC Act constitutes negligence *per se*.

225. The harm that has occurred because of Defendants' conduct is the type of harm that the FTC Act and Part 2 was intended to guard against.

226. As a direct and proximate result of Defendants' negligence, Plaintiffs and the Class Members have been injured as described herein, and is entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

THIRD CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(Plaintiffs on behalf of the Class)

227. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

228. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

229. As a provider of technology services and a recipient of employees and consumers' PII, Defendants have a fiduciary relationship to its employees and consumers, including Plaintiffs and Class members.

230. Because of that fiduciary relationship, Defendants were provided with and stored private and valuable PII related to Plaintiffs and the Class. Plaintiffs and the Class were entitled to expect their information would remain confidential while in Defendants' possession.

231. Defendants owed a fiduciary duty under common law to Plaintiffs and Class Members to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PII in Defendants' possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons.

232. As a result of the parties' fiduciary relationship, Defendants have an obligation to maintain the confidentiality of the information within Plaintiffs' and Class members' PII.

233. Defendants' employees and consumers, including Plaintiffs and Class members, have a privacy interest in personal financial matters, and Defendants have a fiduciary duty not to disclose such personal data.

234. As a result of the parties' relationship, Defendants have possession and knowledge of Plaintiffs' and Class Members' confidential PII, information not generally known.

235. Plaintiffs and Class members did not consent to nor authorize Defendants to release or disclose their PII to unknown criminal actors.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

236. Defendants breached the fiduciary duties owed to Plaintiffs and Class Members by, among other things:

u. mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

v. mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks;

w. failing to design and implement information safeguards to control these risks;

x. failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures;

y. failing to evaluate and adjust its information security program in light of the circumstances alleged herein;

z. failing to detect the breach at the time it began or within a reasonable time thereafter;

aa. failing to follow its own privacy policies and practices published to its consumers; and

bb. failing to adequately train and supervise employees and third-party vendors with access or credentials to systems and databases containing sensitive PII.

237. But for Defendants' wrongful breach of its fiduciary duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

238. As a direct and proximate result of Defendants' negligence, Plaintiffs and Class Members have suffered injuries, including:

cc. Theft of their PII;

dd. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

ee. Costs associated with purchasing credit monitoring and identity theft protection services;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs.

239. As a direct and proximate result of Defendants' breach of its fiduciary duties, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

FOURTH CAUSE OF ACTION
BREACH OF CONFIDENCE
(Plaintiffs on behalf of the Class)

240. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

241. Plaintiffs and Class Members have an interest, both equitable and legal, in the PII about them that was conveyed to, collected by, and maintained by Defendants and that was ultimately accessed or compromised in the Data Breach.

242. As a provider of technology services and a recipient of employees and consumers' PII, Defendants have a fiduciary relationship to its consumers, including Plaintiffs and Class members.

243. Plaintiffs provided Defendants with their personal and confidential PII under both the express and/or implied agreement of Defendants to limit the use and disclosure of such PII.

244. Defendants owed a duty to Plaintiffs to exercise the utmost care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII in its possession from being compromised, lost, stolen, accessed by, misused by, or disclosed to unauthorized persons.

245. As a result of the parties' relationship, Defendants have possession and knowledge of Plaintiffs' and Class Members' confidential PII.

246. Plaintiffs' PII is not generally known to the public and is confidential by nature.

247. Plaintiffs did not consent to nor authorize Defendants to release or disclose their PII to an unknown criminal actor.

248. Defendants breached the duties of confidence owed to Plaintiffs when Plaintiffs' PII was disclosed to unknown criminal hackers.

249. Defendants breached its duties of confidence by failing to safeguard Plaintiffs' and Class Members' PII, including by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that resulted in the unauthorized access and compromise of PII;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

(b) mishandling its data security by failing to assess the sufficiency of its safeguards in place to control these risks; (c) failing to design and implement information safeguards to control these risks; (d) failing to adequately test and monitor the effectiveness of the safeguards' key controls, systems, and procedures; (e) failing to evaluate and adjust its information security program in light of the circumstances alleged herein; (f) failing to detect the breach at the time it began or within a reasonable time thereafter; (g) failing to follow its on privacy policies and practices published to its consumers; (h) storing PII in an unencrypted and vulnerable manner, allowing its disclosure to hackers; and (i) making an unauthorized and unjustified disclosure and release of Plaintiffs' PII to a criminal third party.

250. But for Defendants' wrongful breach of its duty of confidence owed to Plaintiffs and Class Members, their privacy, confidences, and PII would not have been compromised.

251. As a direct and proximate result of Defendants' breach of Plaintiffs' and Class Members' confidences, Plaintiffs and Class Members have suffered injuries, including:

a. Theft of their PII;

b. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

c. Costs associated with purchasing credit monitoring and identity theft protection services;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

f. The imminent and certainly impending injury flowing from the increased risk

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others; and

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data.

252. Additionally, Defendants received payments from Plaintiffs and Class Members for services with the understanding that Defendants would uphold their responsibilities to maintain the confidences of Plaintiffs' and Class Members' PII.

253. Defendants breached the confidence of Plaintiffs and Class Members when they made an unauthorized release and disclosure of their PII and, accordingly, it would be inequitable for Defendants to retain the benefit at Plaintiffs' and Class Members' expense.

254. As a direct and proximate result of Defendants' breach of their duty of confidences, Plaintiffs and the Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

FIFTH CAUSE OF ACTION
INTRUSION UPON SECLUSION/INVASION OF PRIVACY
(Plaintiffs on behalf of the Class)

255. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

256. Plaintiffs had a reasonable expectation of privacy in the PII Defendants mishandled.

257. Defendants' conduct as alleged above intruded upon Plaintiffs and Class Members'

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

seclusion under common law.

258. By intentionally failing to keep Plaintiffs' PII safe, and by intentionally misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants intentionally invaded Plaintiffs and Class Members' privacy by:

a. Intentionally and substantially intruding into Plaintiffs and Class Members' private affairs in a manner that identifies Plaintiffs and Class Members and that would be highly offensive and objectionable to an ordinary person;

b. Intentionally publicizing private facts about Plaintiffs and Class Members, which is highly offensive and objectionable to an ordinary person; and

c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

259. Given the ubiquity of data breaches, Defendant was at least substantially certain that its failure to implement reasonable cybersecurity measures would result in a data breach and the harms done to Plaintiffs as a result.

260. Defendants knew that an ordinary person in Plaintiffs or Class Members' position would consider Defendants' intentional actions highly offensive and objectionable.

261. Defendants invaded Plaintiffs and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by intentionally misusing and/or disclosing their PII without their informed, voluntary, affirmative, and clear consent.

262. Defendants intentionally concealed from and delayed reporting to Plaintiffs and Class members a security incident that misused and/or disclosed their PII without their informed, voluntary, affirmative, and clear consent.

263. The conduct described above was directed at Plaintiffs and Class Members.

264. As a proximate result of such intentional misuse and disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their PII was unduly frustrated and thwarted. Defendants' conduct amounted to a substantial and serious invasion of Plaintiffs' and Class Members' protected privacy interests causing anguish and suffering such that an ordinary person would consider Defendants' intentional actions or inaction highly offensive and objectionable.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

265. In failing to protect Plaintiffs' and Class Members' PII, and in intentionally misusing and/or disclosing their PII, Defendants acted with intentional malice and oppression and in conscious disregard of Plaintiffs and Class Members' rights to have such information kept confidential and private. Plaintiffs, therefore, seek an award of damages on behalf themselves and the Class.

266. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SIXTH CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Plaintiffs on behalf of the Class)

267. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

268. Plaintiffs bring this claim individually and on behalf of the Class.

269. When Plaintiffs and Class members provided their PII to Defendants in exchange for services, they entered into implied contracts with Defendants, under which Defendants agreed to take reasonable steps to protect Plaintiffs' and Class Members' PII, comply with statutory and common law duties to protect their PII, and to timely notify them in the event of a data breach.

270. Defendants solicited and invited Plaintiffs and Class Members to provide their PII as part of Defendants' provision of services. Plaintiffs and Class Members accepted Defendants' offers and provided their PII to Defendants.

271. When entering into implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendants' data security practices complied with its statutory and common law duties to adequately protect Plaintiffs' and Class Members' PII and to timely notify them in the event of a data breach.

272. Defendants' implied promise to safeguard consumers' PII is evidenced by, *e.g.*, the

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

representations in Defendants' Notice of Privacy Practices set forth above.

273. Plaintiffs and Class members paid money to Defendants to receive services. Plaintiffs and Class members reasonably believed and expected that Defendants would use part of those funds to obtain adequate data security. Defendants failed to do so.

274. Plaintiffs and Class Members would not have provided their PII to Defendants had they known that Defendants would not safeguard their PII, as promised, or provide timely notice of a data breach.

275. Plaintiffs and Class Members fully performed their obligations under their implied contracts with Defendants.

276. Defendants breached its implied contracts with Plaintiffs and Class Members by failing to safeguard Plaintiffs and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

277. The losses and damages Plaintiffs and Class Members sustained include, but are not limited to:

a. Theft of their PII;

b. Costs associated with purchasing credit monitoring and identity theft protection services;

c. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

d. Lowered credit scores resulting from credit inquiries following fraudulent activities;

e. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

f. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

g. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

h. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as Defendants fails to undertake appropriate and adequate measures to protect Plaintiffs and Class Members' data; and

i. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

278. As a direct and proximate result of Defendants' breach of contract, Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, in an amount to be proven at trial.

SEVENTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Plaintiffs on behalf of the Class)

279. Plaintiffs restate and reallege the preceding allegations above as if fully alleged herein.

280. Plaintiffs bring this claim individually and on behalf of the Class in the alternative to Plaintiffs' implied contract claim.

281. Upon information and belief, Defendants funds its security measures entirely from

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

its general revenue, including payments made by or on behalf of Plaintiffs and Class Members.

282. As such, a portion of the payments made by or on behalf of Plaintiffs and Class members is to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendants.

283. Plaintiffs and Class members conferred a monetary benefit on Defendants. Specifically, they worked for or purchased services from Defendants and/or their agents and in so doing provided Defendants with their PII. In exchange, Plaintiffs and Class Members should have received from Defendants the services that were the subject of the transaction and have their PII protected with adequate data security.

284. Defendants knew that Plaintiffs and Class Members conferred a benefit which Defendants accepted. Defendants profited from these transactions and used Plaintiffs' and Class Members' PII for business purposes.

285. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs and Class Members' PII. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendants instead calculated to increase their own profits at Plaintiffs' and Class Members' expense by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of the Defendants' decision to prioritize its own profits over the requisite security.

286. Under the principles of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class Members, because Defendants failed to implement appropriate data management and security measures that are mandated by their common law and statutory duties.

287. Defendants failed to secure Plaintiffs' and Class Members' PII and, therefore, did not provide full compensation for the benefit Plaintiffs and Class Members provided.

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

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

289. If Plaintiffs and Class Members knew that Defendants had not reasonably secured their PII, they would not have agreed to provide their PII to Defendants.

290. Plaintiffs and Class Members have no adequate remedy at law.

291. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class Members have suffered injuries, including, but not limited to:

ff. Theft of their PII;

gg. Costs associated with purchasing credit monitoring and identity theft protection services;

hh. Costs associated with the detection and prevention of identity theft and unauthorized use of their PII;

ii. Lowered credit scores resulting from credit inquiries following fraudulent activities;

jj. Costs associated with time spent and the loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach – including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

kk. The imminent and certainly impending injury flowing from the increased risk of potential fraud and identity theft posed by their PII being placed in the hands of criminals;

ll. Damages to and diminution in value of their PII entrusted, directly or indirectly, to Defendants with the mutual understanding that Defendants would safeguard Plaintiffs' and Class Members' data against theft and not allow access and misuse of their data by others;

mm. Continued risk of exposure to hackers and thieves of their PII, which remains in Defendants' possession and is subject to further breaches so long as

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

Defendants fail to undertake appropriate and adequate measures to protect Plaintiffs' and Class Members' data; and

nn. Emotional distress from the unauthorized disclosure of PII to strangers who likely have nefarious intentions and now have prime opportunities to commit identity theft, fraud, and other types of attacks on Plaintiffs and Class Members.

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

293. Defendants should be compelled to disgorge into a common fund or constructive trust, for Plaintiffs' and Class Member's benefit, proceeds that it unjustly received from them. In the alternative, Defendants should be compelled to refund the amounts that Plaintiffs and Class Members overpaid for Defendants' services.

EIGHTH CAUSE OF ACTION
DECLARATORY JUDGMENT
(Plaintiffs on behalf of the Class)

294. Plaintiffs restate and reallege the preceding allegations the paragraphs above as if fully alleged herein.

295. Plaintiffs bring this claim individually and on behalf of the Class.

296. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and granting further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal statutes described in this Complaint.

297. An actual controversy has arisen in the wake of the Data Breach regarding Defendants' present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' PII, and whether Defendants are currently maintaining data security measures adequate to protect Plaintiffs and Class Members from future data breaches that compromise their PII. Plaintiffs and the Class remain at imminent risk of further compromises of

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

their PII will occur in the future.

298. The Court should also issue prospective injunctive relief requiring Defendants to employ adequate security practices consistent with law and industry standards to protect employees' and consumers' PII.

299. Defendants still possess Plaintiffs' and Class Members' PII.

300. To Plaintiffs' knowledge, Defendants have made no announcement or notification that it has remedied the vulnerabilities and negligent data security practices that led to the Data Breach.

301. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial.

302. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendants if an injunction is issued. Among other things, if another data breach occurs at Defendants, Plaintiffs and Class Members will likely continue to be subjected to a heightened, substantial, imminent risk of fraud, identify theft, and other harm described herein. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

303. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiffs and Class Members, along with other consumers whose PII would be further compromised.

304. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring that Defendants implement and maintain reasonable security measures, including but not limited to the following:

a. Engaging third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training its security personnel regarding any new or modified procedures;

d. Purging, deleting, and destroying PII not necessary for its provisions of services in a reasonably secure manner;

e. Conducting regular database scans and security checks; and

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

NINTH CAUSE OF ACTION
Violation of California's Unfair Competition Law ("UCL")
Cal Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of the Plaintiff Cazares and the California Subclass)

305. Plaintiff Cazares restates and realleges the preceding allegations the paragraphs above as if fully alleged herein.

306. Defendants engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

307. Defendants' conduct is unlawful because it violates the California Consumer Privacy Act of 2018, Civ. Code § 1798.100, et seq. (the "CCPA"), and other state data security laws.

308. Defendants stored Plaintiff Cazares and California Subclass Members' PII in its computer systems and knew or should have known it did not employ reasonable, industry standard,

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

and appropriate security measures that complied with applicable regulations and that would have kept Plaintiff Cazares and the California Subclass's PII secure so as to prevent the loss or misuse of that PII.

309. Defendants failed to disclose to Plaintiff Cazares and the California Subclass that their PII was not secure. However, Plaintiff Cazares and the California Subclass were entitled to assume, and did assume, that Defendants had secured their PII. At no time were Plaintiff Cazares and the California Subclass on notice that their PII was not secure, which Defendants had a duty to disclose.

310. Defendants also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff Cazares and the California Subclass' nonencrypted and nonredacted PII.

311. Had Defendants complied with these requirements, Plaintiff Cazares and the California Subclass would not have suffered damage related to the data breach.

312. Defendants' conduct was unlawful, in that it violated the CCPA.

313. Defendants' acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

314. Defendants' conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

315. Defendants' conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

316. Defendants also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendants' acts and omissions thus amount to a violation of the law.

317. Instead, Defendants made Plaintiff Cazares and California Subclass Members' PII accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff Cazares and the California Subclass to an impending risk of identity theft. Additionally, Defendants' conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

318. As a result of those unlawful and unfair business practices, Plaintiffs Cazares and the California Subclass suffered an injury-in-fact and lost money or property.

319. The injuries to Plaintiff Cazares and the California Subclass greatly outweigh any alleged countervailing benefit to consumers or competition under all the circumstances.

320. There were reasonably available alternatives to further Defendants' legitimate business interests, other than the misconduct alleged in this complaint.

321. Therefore, Plaintiff Cazares and the California Subclass are entitled to equitable relief, including restitution of all monies paid to or received by Defendants; disgorgement of all profits accruing to Defendants because of its unfair and improper business practices; a permanent injunction enjoining Defendants' unlawful and unfair business activities; and any other equitable relief the Court deems proper.

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

TENTH CAUSE OF ACTION
Violation of the California Customer Records Act
Cal. Civ. Code § 1798.80, et seq.
(On Behalf of the Plaintiff Cazares and the California Subclass)

322. Plaintiff Cazares restates and realleges the preceding allegations in the paragraphs above as if fully alleged herein.

323. Under the California Customer Records Act, any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" must "disclose any breach of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82. The disclosure must "be made in the most expedient time possible and without unreasonable delay" but disclosure must occur "immediately following discovery [of the breach], if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Id.

324. The Data Breach constitutes a "breach of the security system" of Defendants.

325. An unauthorized person acquired Plaintiff Cazares' and the California Subclass Members' unencrypted PII.

326. Defendants knew that an unauthorized person had acquired Plaintiff Cazares and California Subclass Members' personal, unencrypted PII but waited over a year and a half to notify them. Given the severity of the Data Breach, waiting over a year and a half was an unreasonable delay.

327. Defendants' unreasonable delay prevented Plaintiff Cazares and the California Subclass from taking appropriate measures from protecting themselves against harm.

328. Because Plaintiff Cazares and the California Subclass were unable to protect themselves, they suffered incrementally increased damage that they would not have suffered with timelier notice.

329. Plaintiff Cazares and the California Subclass are entitled to equitable relief and

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

damages in an amount to be determined at trial.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all others similarly situated, pray for relief as follows:

a. For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

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

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

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

e. Ordering Defendants to pay for not less than three years of credit monitoring services for Plaintiffs and the Class;

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

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

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

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

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

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com

JURY TRIAL DEMANDED

A jury trial is demanded by Plaintiffs on all claims so triable.

Dated: December 31, 2024

Respectfully Submitted,

/s/ Samuel J. Strauss

Samuel J. Strauss (SBN 46971)
Raina C. Borrelli*
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
sam@straussborrelli.com
raina@straussborrelli.com

Marc H. Edelson (admitted *Pro Hac Vice*)
EDELSON LECHTZIN LLP
411 S. State Street
Suite N-300
Newtown PA, 18940
Telephone: (215) 867-2399
medelson@edelson-law.com

J. Gerard Stranch, IV*
Andrew E. Mize*
STRANCH, JENNINGS & GARVEY, PLLC
The Freedom Center
223 Rosa L. Parks Avenue, Suite 200
Nashville, Tennessee 37203
Telephone: (615) 254-8801
Facsimile: (615) 255-5419
gstranch@stranchlaw.com
amize@stranchlaw.com

Lynn A. Toops*
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, Indiana 46204
Telephone: (317) 636-6481
ltoops@cohenandmalad.com

** Pro hac vice forthcoming*

Attorneys for Plaintiffs and Proposed Class

STRAUSS BORRELLI PLLC
980 N Michigan Avenue, Suite 1610
Chicago, Illinois 60611-4501
TEL. 872.263.1100 • FAX 872.863.1109
straussborrelli.com