

Exhibit A

JUDGE RICHARD A. JONES

**UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE**

**IN RE: FORTIVE DATA SECURITY
LITIGATION**
THIS DOCUMENT RELATES TO:

CASE NO. 2:24-CV-01668-RAJ

All Actions

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

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

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

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

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

17 We implement and maintain reasonable security appropriate to the nature of the
 18 Personal Information that we collect, use, retain, transfer or otherwise process. Our
 19 reasonable security program is implemented and maintained in accordance with
 20 applicable law and relevant standards as outlined in the report issued by the
 21 California Attorney General in February 2016.²

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

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

26 ¹ <https://investors.fortive.com/company-information>

27 ² Fortive Corp CCPA Public Facing Privacy Notice (20191218bis)

28 ³ ASPS, Privacy Policy, <https://www.asp.com/en-us/privacy-policy#wheredowe> (last visited
 29 October 24, 2024).

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

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

10 8. Defendants’ network experienced two data breaches that occurred between January
 11 25, 2023, and November 6, 2023. Defendants admit that “in October and November 2023, we
 12 detected unusual activity within our network environment stemming from cybersecurity incidents
 13 involving **two** separate unauthorized third parties.” *See* sample Breach Notice attached as Exhibit
 14 A. (emphasis added). The breaches continued for eleven months before Defendants detected them.
 15 Following an internal investigation in or around November 2023, Defendants learned
 16 cybercriminals had gained unauthorized access to employees’ and consumers’ PII. *Id.*

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

23 10. Defendants’ cybersecurity was so inadequate that not only did it take it a year and
 24 half to recognize that cybercriminals had access to its current and former employees and
 25 consumers’ most sensitive information, but, following discovery of the Breach in October 2023,
 26 Defendants struggled to terminate the cybercriminals’ access to their systems until November 6,
 27 2023.

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

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

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

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

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

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

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

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

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

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

11 20. Plaintiffs, on behalf of themselves and others similarly situated, bring claims for
12 negligence, negligence *per se*, breach of fiduciary duty, breach of confidences, intrusion upon
13 seclusion/invasion of privacy, breach of an implied contract, unjust enrichment, declaratory
14 judgment, violation of California’s Unfair Competition Law (“UCL”) Cal Bus. & Prof. Code §
15 17200, *et seq.* and violation of the California Customer Records Act Cal. Civ. Code § 1798.80, *et*
16 *seq.*, seeking actual and putative damages, with attorneys’ fees, costs, and expenses, and
17 appropriate injunctive and declaratory relief.

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

PARTIES

Plaintiff Michael Dudley

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

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

5 **Plaintiff Sherry Dudley**

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

12 **Plaintiff Matthew Spaeth**

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

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

22 **Plaintiff Jennifer Nelson**

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

26 **Plaintiff Seth Toepfer**

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

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

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

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

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

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

13 **Plaintiff Marilyn Cazares**

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

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

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

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

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

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

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

7 **Defendant Fortive Corporation**

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

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

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

20 41. Accruent touts itself to be “the world’s leading provider of workplace and asset
 21 management software for unifying the built environment.”⁴ It boasts an annual revenue of \$270
 22 million.⁵

23 42. Defendant, Advanced Sterilization Products Services Inc., is a New Jersey
 24 corporation, with its principal place of business located at 33 Technology Drive, Irvine, California
 25

26 ⁴ Accruent, <https://www.accruent.com/about-us> (last visited October 14, 2024).

27 ⁵ Zoominfo, Accruent, <https://www.zippia.com/accruent-careers-13439/revenue/> (last visited October 14 2024).

1 92618. ASP is a Fortive operating company.

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

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

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

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

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

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

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

21
 22
 23
 24 ⁶ ASPS, <https://www.asp.com/en-us/about> (last visited October 24, 2024).

25 ⁷ Zoominfo, ASPS, <https://www.zoominfo.com/c/advanced-sterilization-products-inc/590548>
 (last visited October 24, 2024).

26 ⁸ Censis, <https://censis.com/> (last visited October 8, 2024).

27 ⁹Zoominfo, <https://www.zoominfo.com/c/censis-technologies-inc/22827725> (last visited October
 8, 2024).

1 worldwide.”¹⁰ Industrial Scientific boasts a total annual revenue of over \$169.8 million.¹¹

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

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

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

10 JURISDICTION AND VENUE

11 53. This Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. §
 12 1332(d). The amount in controversy in this Class action exceeds \$5,000,000, exclusive of interest
 13 and costs, and there are numerous Class members who are citizens of states other than Defendants’
 14 states of citizenship.

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

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

22 FACTUAL BACKGROUND

23 *Defendants and the Services Provided.*

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

25 ¹⁰ Industrial Scientific, About us, <https://www.indsci.com/en/about> (last visited October 11,
 26 2024).

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

1 with global operations and sales. Established in 2016, as a spin-off from Danaher Corp., the
 2 Defendants have over 18,000 employees with facilities in over 60 countries. Its global revenue in
 3 2023 exceeded \$6 billion.¹²

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

- 6 a. name, residential address, phone number and email address
- 7 b. date of birth
- 8 c. demographic information
- 9 d. Social Security number
- 10 e. tax identification number
- 11 f. financial information
- 12 g. medication information
- 13 h. health insurance information
- 14 i. photo identification
- 15 j. employment information, and
- 16 k. other information that Defendants may deem necessary to provide its services.

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

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

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

26 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, 27 2024).

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

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

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

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

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

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

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

17 66. In tandem with the increase in data breaches, the rate of identity theft complaints
 18 has also increased over the past few years. For instance, in 2017, 2.9 million people reported some
 19 form of identity fraud compared to 5.7 million people in 2021.¹³

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

23
 24
 25 ¹³ *Insurance Information Institute, Facts + Statistics: Identity theft and cybercrime*, Insurance
 26 Information Institute, <https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime#Identity%20Theft%20And%20Fraud%20Reports,%202015-2019%20> (last visited
 27 Apr. 17, 2023).

1 68. PII is a valuable property right.¹⁴ The value of PII as a commodity is measurable.¹⁵
 2 “Firms are now able to attain significant market valuations by employing business models
 3 predicated on the successful use of personal data within the existing legal and regulatory
 4 frameworks.”¹⁶ American companies are estimated to have spent over \$19 billion on acquiring
 5 personal data of consumers in 2018.¹⁷ It is so valuable to identity thieves that once PII has been
 6 disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for many years.

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

13 70. According to the U.S. Government Accountability Office, which conducted a study
 14 regarding data breaches: “[I]n some cases, stolen data may be held for up to a year or more before
 15 being used to commit identity theft. Further, once stolen data has been sold or posted on the [Dark]
 16 Web, fraudulent use of that information may continue for years. As a result, studies that attempt to
 17
 18

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

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

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

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

1 measure the harm resulting from data breaches cannot necessarily rule out all future harm.”¹⁸

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

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

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

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

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

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

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

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

27 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>.

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

7 76. To date, Defendants investigation has determined that the private information of
8 roughly 31,000 current and former employees, customers and other affiliated individuals was
9 accessed and compromised by unauthorized users on two separate occasions between January 25,
10 2023, and November 6, 2023.

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

- a. Accrue: 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;

²⁷ ²⁸ See Maine Consumer Protection Bureau Notice, ftv-employment-20241003, mm.nh.gov (last visited October 10, 2024).

1. Dynapar Corporation: number of individuals impacted currently unknown;
2. m. Fluke Biomedical: number of individuals impacted currently unknown;
3. n. Global Physics Solutions: number of individuals impacted currently unknown;
4. o. Intelex Technologies US: number of individuals impacted currently unknown;
5. p. Provation Software: number of individuals impacted currently unknown;
6. q. Qualitrol Company: number of individuals impacted currently unknown;
7. r. ServiceChannel.com Inc.: number of individuals impacted currently unknown;
8. s. Tektronix In.: number of individuals impacted currently unknown;
9. t. Janos Technology: number of individuals impacted currently unknown.

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

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

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



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

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

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

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

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

25 85. Upon information and belief, and based on the type of cyberattack, it is plausible
 26 and likely that Plaintiffs' PII was stolen in the Data Breach. Plaintiffs further believe their PII was
 27

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

23 22 *Start with Security – A Guide for Business*, United States Federal Trade Comm’n (2015),
 24 <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf>.

25 23 *Protecting Personal Information: A Guide for Business*, United States Federal Trade Comm’n,
 26 https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personalinformation.pdf.

27 24 *Id.*

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

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

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

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

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

23 101. Theft of PII is serious. The FTC warns consumers that identity thieves use PII to
24 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>.

1 and credit in a person's name.

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

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

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

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

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

23
 24 ²⁶See *IdentityTheft.gov*, Federal Trade Commission, <https://www.identitytheft.gov/Steps> (last accessed Feb. 24, 2023).

25 ²⁷See, e.g., John T. Soma, et al., *Corporate Privacy Trend: The “Value” of Personally Identifiable*
 26 *Information (“PII”) Equals the “Value” of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4
 27 (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)).

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

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

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

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

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

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

24 28 See, e.g., Christine DiGangi, *5 Ways an Identity Thief Can Use Your Social Security Number*
 25 (Nov. 2, 2017), <https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/> (emphasis added).

26 29 *Id.*

27 30 *Id.*

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

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

12 112. This was a financially motivated Data Breach, as the only reason the cybercriminals
 13 go through the trouble of running a targeted cyberattack against companies like Fortive is to get
 14 information that they can monetize by selling on the black market for use in the kinds of criminal
 15 activity described herein. This data demands a much higher price on the black market. Martin
 16 Walter, senior director at cybersecurity firm RedSeal, explained, “[c]ompared to credit card
 17 information, personally identifiable information and Social Security Numbers are worth more than
 18 10x on the black market.”

19 113. Indeed, a Social Security number, date of birth, and full name can sell for \$60 to
 20 \$80 on the digital black market.³³ “[I]f there is reason to believe that your personal information
 21 has been stolen, you should assume that it can end up for sale on the dark web.”³⁴

22 ³¹ *Id.* at 4.

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

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

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

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

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

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

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

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

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

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

21 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.

22 ³⁵ *Id.*

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

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

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

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

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

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

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

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

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

26
 27 ³⁹ *Id.*

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

7 ***Plaintiffs Michael Dudley and Sherry Dudley's Experience and Injuries***

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

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

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

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

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

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

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

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

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

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

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

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

17 ***Plaintiff Matthew Spaeth's Experience and Injuries***

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

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

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

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

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

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

1 his rights to privacy.

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

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

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

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

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

25 150. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is
 26 here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather
 27

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

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

6 ***Plaintiff Jennifer Nelson's Experience and Injuries***

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

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

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

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

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

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

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

26
 27 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).

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

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

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

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

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

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

18 ***Plaintiff Seth Toepfer's Experience and Injuries***

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

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

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

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

26 41 What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-do->
 27 [hackers-do-with-stolen-information](https://www.aura.com/learn/what-do-hackers-do-with-stolen-information) (last visited January 9, 2024).

1 violates his rights to privacy.

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

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

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

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

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

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

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

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

6 ***Plaintiff Marilyn Cazares's Experience and Injuries***

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

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

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

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

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

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

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

26 42 What do Hackers do with Stolen Information, Aura, <https://www.aura.com/learn/what-do->
 27 [hackers-do-with-stolen-information](https://www.aura.com/learn/what-do-hackers-do-with-stolen-information) (last visited January 9, 2024).

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

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

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

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

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

21 ***Plaintiffs Suffered Damages.***

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

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

26 27 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).

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

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

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

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

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

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

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

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

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

17 195. In addition, Plaintiffs and Class Members have suffered emotional distress because
18 of the Data Breach, the increased risk of identity theft and financial fraud, and the unauthorized
19 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).

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

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

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

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

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

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

- 22 a. Whether Defendants failed to timely notify Plaintiffs and Class Members of the
 Data Breach;
- 23 b. Whether Defendants have a duty to protect Plaintiffs' and Class Members' PII;
- 24 c. Whether Defendants were negligent in collecting and storing Plaintiffs and
 Class Members' PII, and breached their duties thereby;
- 25 d. Whether Defendants breached their fiduciary duty to Plaintiffs and the Class;

- 1 e. Whether Defendants breached their duty of confidence to Plaintiffs and the
- 2 Class;
- 3 f. Whether Defendants violated their own Privacy Practices;
- 4 g. Whether Defendants entered a contract implied in fact with Plaintiffs and the
- 5 Class;
- 6 h. Whether Defendants breached that contract by failing to adequately safeguard
- 7 Plaintiffs and Class members' PII;
- 8 i. Whether Defendants were unjustly enriched;
- 9 j. Whether Plaintiffs and Class Members are entitled to damages as a result of
- 10 Defendants' wrongful conduct; and
- 11 k. Whether Plaintiffs and Class Members are entitled to restitution as a result of
- 12 Defendants' wrongful conduct.

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

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

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

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

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

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

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

- 18 a. Whether Defendants failed to timely and adequately notify the public of the
 Data Breach;
- 19 b. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise
 due care in collecting, storing, and safeguarding their PII;
- 20 c. Whether Defendants' security measures to protect its data systems were
 reasonable in light of best practices recommended by data security experts;
- 21 d. Whether Defendants' failure to institute adequate protective security measures
 amounted to negligence;
- 22 e. Whether Defendants failed to take commercially reasonable steps to safeguard
 employee and consumer PII; and

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

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

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

- 2 a. mismanaging its system and failing to identify reasonably foreseeable
3 internal and external risks to the security, confidentiality, and integrity of
4 customer information that resulted in the unauthorized access and
5 compromise of PII;
- 6 b. mishandling its data security by failing to assess the sufficiency of its
7 safeguards in place to control these risks;
- 8 c. failing to design and implement information safeguards to control these
9 risks;
- 10 d. failing to adequately test and monitor the effectiveness of the safeguards'
11 key controls, systems, and procedures;
- 12 e. failing to evaluate and adjust its information security program in light of the
13 circumstances alleged herein;
- 14 f. failing to detect the breach at the time it began or within a reasonable time
15 thereafter;
- 16 g. failing to follow its own privacy policies and practices published to its
17 employees and consumers; and
- 18 h. failing to adequately train and supervise employees and third-party vendors
19 with access or credentials to systems and databases containing sensitive PII.

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

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

- 24 a. Theft of their PII;
- 25 b. Costs associated with the detection and prevention of identity theft and
26 unauthorized use of their PII;
- 27 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 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.

**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.

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

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

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

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

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

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

**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.

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

- 3 u. mismanaging its system and failing to identify reasonably foreseeable internal and
 4 external risks to the security, confidentiality, and integrity of customer information
 5 that resulted in the unauthorized access and compromise of PII;
- 6 v. mishandling its data security by failing to assess the sufficiency of its safeguards in
 7 place to control these risks;
- 8 w. failing to design and implement information safeguards to control these risks;
- 9 x. failing to adequately test and monitor the effectiveness of the safeguards' key
 10 controls, systems, and procedures;
- 11 y. failing to evaluate and adjust its information security program in light of the
 12 circumstances alleged herein;
- 13 z. failing to detect the breach at the time it began or within a reasonable time
 14 thereafter;
- 15 aa. failing to follow its own privacy policies and practices published to its consumers;
 16 and
- 17 bb. failing to adequately train and supervise employees and third-party vendors with
 18 access or credentials to systems and databases containing sensitive PII.

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

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

- 23 cc. Theft of their PII;
- 24 dd. Costs associated with the detection and prevention of identity theft and
 25 unauthorized use of their PII;
- 26 ee. Costs associated with purchasing credit monitoring and identity theft protection
 27 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' 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.

**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;

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

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

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

- 14 a. Theft of their PII;
- 15 b. Costs associated with the detection and prevention of identity theft and
 unauthorized use of their PII;
- 16 c. Costs associated with purchasing credit monitoring and identity theft protection
 services;
- 17 d. Lowered credit scores resulting from credit inquiries following fraudulent
 activities;
- 18 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;
- 19 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; 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'

1 seclusion under common law.

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

- 5 a. Intentionally and substantially intruding into Plaintiffs and Class Members'
 6 private affairs in a manner that identifies Plaintiffs and Class Members and that
 7 would be highly offensive and objectionable to an ordinary person;
- 8 b. Intentionally publicizing private facts about Plaintiffs and Class Members,
 9 which is highly offensive and objectionable to an ordinary person; and
- 10 c. Intentionally causing anguish or suffering to Plaintiffs and Class Members.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 15 a. Theft of their PII;
- 16 b. Costs associated with purchasing credit monitoring and identity theft
 protection services;
- 17 c. Costs associated with the detection and prevention of identity theft and
 unauthorized use of their PII;
- 18 d. Lowered credit scores resulting from credit inquiries following fraudulent
 activities;
- 19 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;

- 1 f. The imminent and certainly impending injury flowing from the increased
- 2 risk of potential fraud and identity theft posed by their PII being placed in
- 3 the hands of criminals;
- 4 g. Damages to and diminution in value of their PII entrusted, directly or
- 5 indirectly, to Defendants with the mutual understanding that Defendants
- 6 would safeguard Plaintiffs' and Class Members' data against theft and not
- 7 allow access and misuse of their data by others;
- 8 h. Continued risk of exposure to hackers and thieves of their PII, which
- 9 remains in Defendants' possession and is subject to further breaches so long
- 10 as Defendants fails to undertake appropriate and adequate measures to
- 11 protect Plaintiffs and Class Members' data; and
- 12 i. Emotional distress from the unauthorized disclosure of PII to strangers who
- 13 likely have nefarious intentions and now have prime opportunities to
- 14 commit identity theft, fraud, and other types of attacks on Plaintiffs and
- 15 Class Members.

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

19
 20 **SEVENTH CAUSE OF ACTION**
 21 **UNJUST ENRICHMENT**
 22 **(Plaintiffs on behalf of the Class)**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

6 ff. Theft of their PII;

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

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

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

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

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

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

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

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

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

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

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

12

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

14

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

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

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

22 297. An actual controversy has arisen in the wake of the Data Breach regarding
 23 Defendants' present and prospective common law and other duties to reasonably safeguard
 24 Plaintiffs' and Class Members' PII, and whether Defendants are currently maintaining data security
 25 measures adequate to protect Plaintiffs and Class Members from future data breaches that
 26 compromise their PII. Plaintiffs and the Class remain at imminent risk of further compromises of
 27

1 their PII will occur in the future.

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

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

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

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

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

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

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

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

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,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

23

24

25

26

27

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)

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

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

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

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

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

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

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

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

1 damages in an amount to be determined at trial.

2 **PRAYER FOR RELIEF**

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

- 5 a. For an Order certifying this action as a Class action and appointing Plaintiffs as
6 Class Representatives and their counsel as Class Counsel;
- 7 b. For equitable relief enjoining Defendants from engaging in the wrongful
8 conduct complained of herein pertaining to the misuse and/or disclosure of
9 Plaintiffs' and Class Members' PII, and from refusing to issue prompt, complete
10 and accurate disclosures to Plaintiffs and Class Members;
- 11 c. For equitable relief compelling Defendants to utilize appropriate methods and
12 policies with respect to consumer data collection, storage, and safety, and to
13 disclose with specificity the type of Personal Information compromised during
14 the Data Breach;
- 15 d. For equitable relief requiring restitution and disgorgement of the revenues
16 wrongfully retained as a result of Defendants' wrongful conduct;
- 17 e. Ordering Defendants to pay for not less than three years of credit monitoring
18 services for Plaintiffs and the Class;
- 19 f. For an award of actual damages, compensatory damages, statutory damages,
20 and statutory penalties, in an amount to be determined, as allowable by law;
- 21 g. For an award of punitive damages, as allowable by law;
- 22 h. For an award of attorneys' fees and costs, and any other expense, including
23 expert witness fees;
- 24 i. Pre- and post-judgment interest on any amounts awarded; and,
- 25 j. Such other and further relief as this court may deem just and proper.

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

1 * *Pro hac vice forthcoming*
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27

Attorneys for Plaintiffs and Proposed Class

— EXHIBIT A —

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

Dear [REDACTED]

At [REDACTED], we value and respect the privacy of your information, which is why we are writing to inform you about recent cybersecurity incidents that involved personal information. We want to provide you with further information about these incidents, the measures taken in response, and steps that you can take to help protect yourself.

WHAT HAPPENED?

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 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 [REDACTED] Once our comprehensive investigation was concluded, we worked to notify you as quickly as we could.

WHAT INFORMATION WAS INVOLVED?

Based on our subsequent investigation and comprehensive review of potentially affected data, we determined that the information involved in these incidents may have included your full name, and one or more of the following: date of birth, Social Security number, driver's license or state-issued identification card number, passport number, birth certificate number, financial account number, credit or debit card number, and/or health insurance information.

WHAT HAVE WE DONE IN RESPONSE?

In response to the incidents, we promptly implemented remedial and containment measures, working with leading external cybersecurity experts to assist with these efforts. In addition, we notified U.S. federal law enforcement and enhanced our security monitoring capabilities and technical controls. In addition to those efforts, we have arranged for you to enroll, at no cost to you, in a comprehensive 24-month credit monitoring and identity restoration service through Equifax. A description of this service and instructions on how to enroll can be found within the enclosed "Other Important Information" document included with this letter.

WHAT YOU CAN DO NOW?

Please review the enclosed "Other Important Information" document for further steps you can take to protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection, as well as details on how to place a fraud alert or a security freeze on your credit file. We recommend that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports for unauthorized activity. If you discover any suspicious or unusual activity on your accounts, promptly notify the financial institution or company with which your account is maintained.

FOR MORE INFORMATION.

For further information and assistance, please contact our dedicated incident response line at 833-251-9667 between 9 a.m. – 9 p.m. EST, Monday through Friday.

Sincerely,

[REDACTED]

OTHER IMPORTANT INFORMATION**Enroll in Credit Monitoring**

Enter your Activation Code: [REDACTED]

Enrollment Deadline: [REDACTED]

Equifax Complete™ Premier

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts⁴, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁶.
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

Enrollment Instructions

Go to www.equifax.com/activate

Enter your unique Activation Code of [REDACTED] then click “Submit” and follow these 4 steps:

1. Register:

Complete the form with your contact information and click “Continue”.

If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.

Once you have successfully signed in, you will skip to the Checkout Page in Step 4

2. Create Account:

Enter your email address, create a password, and accept the terms of use.

3. Verify Identity:

To enroll in your product, we will ask you to complete our identity verification process.

4. Checkout:

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

You’re done!

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

¹The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

²Credit monitoring from Experian and TransUnion will take several days to begin. ³WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded. ⁴The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. ⁵Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.co ⁶The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Free Credit Report. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the nationwide credit reporting agencies. To order your annual free credit report please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's (FTC) website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Contact information for the national credit reporting agencies for the purpose of requesting a copy of your credit report and other general inquiries is provided below:

- **Equifax**, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- **Experian**, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213
- **Innovis**, PO Box 1689, Pittsburgh, PA 15230-1689, www.innovis.com, 1-800-540-2505

Fraud Alert. You have the right to place an initial or extended “fraud alert” on your file at no cost by contacting any of the nationwide credit reporting agencies. Contact information for the national credit reporting agencies for the purposes of placing a fraud alert on your file is provided below. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert displayed on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. For this reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. If you are a victim of identity theft and have filed an identity theft report with law enforcement, you may want to consider placing an extended fraud alert, which lasts for 7 years, on your credit file.

- **Equifax**, PO Box 105069, Atlanta, GA 30348-5069, www.equifax.com/personal/credit-report-services/credit-fraud-alerts, 1-800-525-6285
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/fraud/center.html, 1-888-397-3742
- **TransUnion**, PO Box 2000, Chester, PA 19016, www.transunion.com/fraud-alerts, 1-800-680-7289
- **Innovis Consumer Assistance**, PO Box 26, Pittsburgh, PA 15230-0026, www.innovis.com/personal/fraudActiveDutyAlerts, 1-800-540-2505

Security Freeze. You have the right to place, lift, or remove a “security freeze” on your credit report, free of charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You must place your request for a freeze separately with each of the consumer reporting agencies. To place a security freeze on your credit report, you may do so by contacting each of the consumer reporting agencies through the contact information below:

- **Equifax**, PO Box 105788, Atlanta, GA 30348-5788, www.equifax.com/personal/credit-report-services/credit-freeze, 1-800-298-0045
- **Experian**, PO Box 9554, Allen, TX 75013, www.experian.com/freeze/center.html, 1-888-397-3742
- **TransUnion**, PO Box 160, Woodlyn, PA 19094, www.transunion.com/credit-freeze, 1-888-909-8872
- **Innovis**, PO Box 26, Pittsburgh, PA 15230-0026, www.innovis.com/personal/securityFreeze, 1-800-540-2505

In order to request a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or up to 3 business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within 5 business days and may provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have 1 business day after receiving your request by toll-free telephone or secure electronic means, or 3 business days after receiving your request by mail, to remove the security freeze.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the FTC, proper law enforcement authorities and/or your state attorney general. You may also contact these agencies for information on how to prevent or avoid identity theft and to obtain additional information about fraud alerts and security freezes. You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (438-4338).

- **For California residents**, you may also wish to review the information provided by the California Attorney General at <https://oag.ca.gov/idtheft>.
- **For District of Columbia residents**, you may also obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.
- **For Iowa Residents**, you are advised to report suspected incidents of identity theft to law enforcement or the Iowa Attorney General's Office at Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, telephone: 1-515-281-5926 or 1-888-777-4590.
- **For Maryland residents**, you may obtain information about avoiding identity theft from the Maryland Office of the Attorney General at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [https://www.marylandattorneygeneral.gov](http://www.marylandattorneygeneral.gov).
- **For New Mexico residents**, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.
- **For New York residents**, you may obtain additional information about security breach response and identity theft prevention and protection from the New York State Office of the Attorney General by calling 1-800-771-7755 or visiting <https://ag.ny.gov>; the New York State Police by calling 1-518-457-6721 or visiting <https://troopers.ny.gov/>; and/or the New York Department of State by calling 1-800-697-1220 or visiting <https://www.dos.ny.gov>.

- **For North Carolina residents**, you may obtain additional information about preventing identity theft provided by the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.
- **For Oregon Residents**, you are advised to report any suspected incidents of identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at <https://doj.state.or.us>, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.
- **For Rhode Island residents**, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to the incidents. There are approximately [REDACTED] Rhode Island residents that may be impacted by the incidents.