IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

Leo Guy, Ryan Tanner, Magaly Granados, Kerry Lamons, Tammy Rano, Vicki Will, and Jennifer White, individually and on behalf all others similarly situated,

Plaintiffs,

v.

CONVERGENT OUTSOURCING, INC.,

Defendant.

Case No. 2:22-cv-01558-MJP

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

JURY DEMAND

Plaintiffs Leo Guy, Ryan Tanner, Magaly Granados, Kerry Lamons, Tammy Rano, Vicki Will, and Jennifer White ("Plaintiffs") bring this action, individually and on behalf of all others similarly situated, against Defendant Convergent Outsourcing, Inc. ("Convergent" or "Defendant"). Plaintiffs seek to obtain damages, restitution, and injunctive relief for a class of individuals ("Class" or "Class Members") who are similarly situated and have received notices of the data breach from Convergent. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

I. NATURE OF THE ACTION

1. This class action arises out of a 2022 data breach ("Data Breach") of documents and information stored on the computer network of Convergent, a third-party consumer debt collection company that serves the telecommunication, utility, banking, cable company, and financial service industries.[1]

2. According to its website, "Convergent believe[s] in customer service"[2] and claims "[they] want to make it easy as possible for people to pay the debts they owe."[3]

3. On its computer network, Convergent holds and stores certain highly sensitive personally identifiable information ("PII" or "Private Information") of Plaintiffs and the putative Class Members, who are customers of companies for which Convergent provides debt collection services, i.e., individuals who provided their highly sensitive and private information in exchange for business services.

4. According to the Notice of Data Breach letter ("Notice Letter") that Convergent sent to Plaintiffs and Class Members, Convergent first became aware of the Data Breach on June 17, 2022, and subsequently launched an investigation, from which it determined that the names, contact information, financial account numbers, and Social Security numbers of Plaintiff and Class Members were accessed by an unauthorized individual.[4]

5. Despite the substantial harm that would result to Plaintiffs and Class Members as a result of the Data Breach, Convergent waited more than 4 months to begin notifying victims. And even then, Convergent downplayed the seriousness of the incident, stating only that Convergent had become aware of an "interruption to certain services performed by Convergent

---

[1] https://www.convergentusa.com/outsourcing/question/list?type=A (last accessed January 26, 2023).

[2] https://www.convergentusa.com/outsourcing/site/who-is-convergent-outsourcing (last accessed on January 26, 2023).

[3] *Id.*

[4] *See* Exhibit A, Plaintiff Guy's Notice Letter.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

affecting certain computer systems."[5]

6. Rather than use plain language to alert Plaintiffs and Class Members as to the gravity of the situation, Convergent confoundingly admitted that "an external actor gained unauthorized access to our systems and deployed a ransomware malware" and that its "investigation also revealed that the unauthorized actor deployed certain data extraction tools on one storage drive that is used to save and share files internally."[6]

7. As a result of Convergent's Data Breach, Plaintiffs and thousands (if not more) of Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

8. In addition, Plaintiffs' and Class Members' sensitive Private Information—which they entrusted to Defendant—was compromised and unlawfully accessed and extracted during the Data Breach. Indeed, Defendant claimed in the Notice Letter that "[they] take the confidentiality, privacy, and security of information in our care seriously"[7]

9. Based upon Convergent's Notice Letter, the Private Information compromised in the Data Breach was intentionally accessed and exfiltrated, by the cyber-criminals who perpetrated this attack, and this Private Information remains in the hands of those cyber-criminals.

10. The Data Breach was a direct result of Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect Plaintiffs' and Class Members' Private Information.

11. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that

---

[5] *Id.*
[6] *Id.*
[7] *Id.*

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

Defendant collected and maintained, and to address Defendant's failure to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access of an unknown third party and precisely what specific type of information was accessed.

12. Defendant maintained the Private Information in a reckless manner. In particular, Defendant maintained the Private Information on Defendant's computer network in a condition vulnerable to cyberattacks. The mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant. Thus, Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

13. Defendant disregarded the privacy and property rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt, accurate, and complete notice of the Data Breach.

14. In addition, Defendant and its employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant properly monitored its computers, it would have discovered the intrusion sooner, and potentially been able to prevent or mitigate the injuries to Plaintiffs and the Class.

15. Plaintiffs' and Class Members' identities are now at present and continued risk as a result of Defendant's negligent conduct because the Private Information (including Social Security numbers) that Defendant collected and maintained for its own pecuniary benefit is now in the hands of data thieves.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

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

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

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

19. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during the Data Breach (the "Class").

20. Accordingly, Plaintiffs bring this action against Defendant for negligence, negligence per se, breach of implied contract, breach of confidence, invasion of privacy, unjust enrichment, declaratory judgment, breach of the Washington Consumer Protection Act, breach of the Washington Data Breach Disclosure Law, and violations of the California Consumer Privacy Act, California UCL, and California's constitutional right to privacy. Plaintiffs seek redress for Convergent's unlawful conduct.

21. Plaintiffs seek remedies including, but not limited to, compensatory and statutory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems (which continue to house the Private Information of Plaintiffs

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

and Class Members), future annual audits, and adequate, long term credit monitoring services funded by Defendant, and declaratory relief.

II. PARTIES

22. Plaintiff Leo Guy is a resident and citizen of the State of New Hampshire.

23. Plaintiff Ryan Tanner is a resident and citizen of the State of Minnesota.

24. Plaintiff Magaly Granados is a resident and citizen of the State of Florida.

25. Plaintiff Kerry Lamons is a resident and citizen of the State of California.

26. Plaintiff Tammy Rano is a resident and citizen of the State of Maine.

27. Plaintiff Vicki Will is a resident and citizen of the State of Nevada.

28. Plaintiff Jennifer White is a resident and citizen of the State of California.

29. Defendant Convergent Outsourcing, Inc., is a Washington for-profit corporation. Convergent's principal place of business is located at 800 SW 39th Street, Suite 100, Renton, Washington 98057. Defendant's registered agent is: CT Corporation System, 711 Capitol Way South, Suite 204, Olympia, Washington 98501.

30. According to its Notice Letter, the business operations of Convergent's affiliate, Account Control Technology, Inc. ("ACT") were also affected by the same Data Breach.[8] Upon information and belief, both Convergent and ACT are subsidiaries of Account Control Technology Holdings, Inc.[9]

31. All of Plaintiffs' claims stated herein are asserted against Defendant Convergent, and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

32. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or

---

[8] *Id.*

[9] https://accountcontrol.com/About-Us/History (last accessed November 1, 2022).

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one member of the class is a citizen of a state different from Defendant.

33. The Court has general personal jurisdiction over Defendant because, personally or through its agents, Defendant operates, conducts, engages in, or carries on a business or business venture in Washington; it is registered with the Secretary of State in Washington as a for-profit corporation; it maintains its headquarters in Washington; and committed tortious acts in Washington.

34. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because it is the district within which Convergent has the most significant contacts.

IV. STATEMENT OF FACTS

Nature of Defendant's Business

35. Convergent started its business as a debt collection agency in 1950. Convergent has approximately 1,000 employees globally in the United States, Asia, Europe, and Africa while maintaining its headquarters in Renton, Washington.[10]

36. As a necessary part of its business collecting consumer debt, Convergent collects Private Information of consumers from companies seeking Convergent's debt collection services. This Private Information includes, *inter alia,* consumers' names, contact information, Social Security numbers, and financial account information.

37. Convergent, in the regular course of its business, collects and maintains the Private Information of consumers (on behalf of its customers) as a requirement of its business practices.

38. Consumers entrusted the customers of Convergent with their Private Information with the mutual understanding that this highly sensitive private information was confidential and

[10] https://www.zoominfo.com/pic/convergent-outsourcing/9502974 (last accessed November 1, 2022).

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

would be properly safeguarded from misuse and theft. Plaintiffs and Class Members would not have allowed Convergent to possess or maintain their Private Information had Convergent disclosed the inadequacy of its data security practices.

39. Convergent promises in its Privacy Policy that they "incorporate commercially reasonable safeguards to help protect and secure your Personal Information."[11]

40. In its California Online Privacy Policy, Convergent acknowledges that it is susceptible to data breaches and ransomware threats, and that it must "detect security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, and prosecuting those responsible for that activity."[12] Moreover, Convergent is aware that it must: comply with federal, state, and local laws; protect the safety, rights, property or security of consumers and third parties; and detect, prevent, or otherwise address fraud, security, or technical issues.[13]

41. In the course of collecting Private Information from consumers, including Plaintiffs and Class Members, Convergent promised to provide confidentiality and adequate security for Private Information through its applicable Privacy Policy and in compliance with statutory privacy requirements applicable to the servicing industry.

42. In its Notice Letters to Plaintiffs and Class Members, Convergent claims that "the confidentiality, privacy, and security of information in our care are among our highest priorities."[14]

43. Plaintiffs and the Class Members, as consumers, relied on the promises and duties of Convergent to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Consumers, in general, demand that businesses that require highly sensitive

---

[11] https://www.convergentusa.com/outsourcing/page/privacy-policy (last accessed on November 1, 2022).

[12] https://www.convergentusa.com/outsourcing/page/ccpa-policy (last accessed on November 1, 2022).

[13] *Id.*

[14] *See* Notice Letter, Ex. A.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

Private Information will provide necessary security to safeguard their Private Information, especially when Social Security numbers are involved.

44. In the course of their dealings, Plaintiffs and Class Members provided Convergent (either directly or through Convergent's business customers) with all or most of the following types of Private Information:

- First and last names;
- Home addresses;
- Email addresses;
- Phone numbers;
- Social Security numbers;
- Employers;
- Account numbers; and
- Bank account or payment card information.[15]

45. Convergent had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII from unauthorized disclosure to third parties.

The Data Breach

46. According to its Notice Letters, on June 17, 2022, Convergent "became aware of an interruption to certain services." After an unspecified amount of time, between the date it "became aware" and the date it sent the Notice Letters, its investigation determined that an "unauthorized actor" accessed the Convergent network and "deployed certain extraction tools on one storage drive that is used to save and share files internally."[16]

[15] *See id.*; *see also* https://www.convergentusa.com/outsourcing/page/privacy-policy (last accessed on January 26, 2023).

[16] Notice Letter, Ex. A.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

47. The Notice Letter does not identify how long before detection the "interruption" was occurring.[17]

48. By October 26, 2022, according to Convergent's own Notice Letters, it was aware that the Data Breach included "name[s], contact information, financial account number[s], Social Security number[s],"[18] including that of Plaintiffs. Convergent does not explain why it waited to send the Notice Letters until over 4 months had passed. This was time that Plaintiffs and Class members could have used to help mitigate the damages they suffered from Convergent's Data Breach.

49. Convergent notified various State Attorney Generals of this Data Breach on or about October 26, 2022, admitting that the Data Breach compromised the Private Information of **640,906** individuals.[19]

50. Convergent has not explained why it failed to expeditiously report the Data Breach within the time constraints required by various state's laws.[20]

51. As a result of Convergent's delay, ***Plaintiffs' and Class Members' Private Information was in the hands of cybercriminals for over 4 months before they were notified*** of Convergent's Data Breach. Time is of the essence when trying to protect against identity theft after a data breach, so early notification is critical.

52. Because of this targeted, intentional cyberattack, data thieves were able to gain access to and obtain data from Convergent that included the Private Information of Plaintiffs and Class Members.

---

[17] *Id.*

[18] *Id.*

[19] https://apps.web.maine.gov/online/aeviewer/ME/40/b5be3a2c-d7bd-4b77-83da-d85b55f9dfe8.shtml (last accessed on January 26, 2023).

[20] *See, e.g.*, Maine's requirements at https://www.maine.gov/ag/consumer/identity_theft/index.shtml (last accessed on January 26, 2023).

53. Convergent admits that the files exfiltrated from Convergent contained at least the following information of Plaintiffs and Class Members: names, contact information, financial account numbers, and Social Security numbers.

54. Upon information and belief, the Private Information stored on Convergent's network was not encrypted because if it had been, the data thieves would have exfiltrated only unintelligible data.

55. Plaintiffs' Private Information was accessed and stolen in the Data Breach. Plaintiffs reasonably believe their stolen Private Information is currently available for sale on the Dark Web because that is the *modus operandi* of cybercriminals who target businesses that collect highly sensitive Private Information.

56. As a result of the Data Breach, Convergent now encourages Class Members to enroll in credit monitoring, fraud consultation, and identity theft restoration services, a tacit admission of the present and continued risk of identity theft that Plaintiffs and Class Members now face.[21]

57. That Convergent is encouraging Plaintiffs and Class Members to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted consumers are subject to a substantial and imminent threat of fraud and identity theft.

58. Convergent had obligations created by contract, industry standards, and common law to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

59. Convergent could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

[21] Notice Letter, Exhibit A.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

Defendant Acquires, Collects, and Stores Plaintiffs' and Class Members' Private Information

60. Convergent acquires, collects, and stores a massive amount of Private Information of consumers for its business purposes as it provides debt collection services to third-party businesses (*i.e.,* Convergent's customers). Upon information and belief, Convergent appears to retain,, rather than properly delete or destroy the Private Information and records of its former customers or of its consumers whose debts have been fully satisfied.

61. By obtaining, collecting, and using Plaintiffs' and Class Members' Private Information for its own financial gain and business purposes, Defendant assumed legal and equitable duties and knew that it was responsible for protecting Plaintiffs' and Class Members' Private Information from disclosure.

62. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Convergent or anyone in Convergent's position had they known of Convergent's lax data security practices.

63. Plaintiffs and the Class Members relied on Defendant to keep their Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

The Data Breach Was Foreseeable

64. It is well known that Private Information, including Social Security numbers in particular, is a valuable commodity and a frequent, intentional target of cyber criminals. Companies that collect such information, including Convergent, are well-aware of the risk of being targeted by cybercriminals.

65. Individuals place a high value not only on their Private Information, but also on the privacy of that data. Identity theft victims suffer severe negative consequences, as well as severe distress and hours of lost time trying to fight against the impact of identity theft.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

66. A data breach increases the risk of becoming a victim of identity theft. Victims of identity theft can suffer from both direct and indirect financial losses. According to a research study published by the Department of Justice, "[a] direct financial loss is the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. It includes both out-of-pocket loss and any losses that were reimbursed to the victim. An indirect loss includes any other monetary cost caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses that are not reimbursed (e.g., postage, phone calls, or notary fees). All indirect losses are included in the calculation of out-of-pocket loss."[22]

67. Individuals, like Plaintiffs and Class members, are particularly concerned with protecting the privacy of their Social Security numbers, because Social Security numbers are the key to stealing any person's identity and can be likened to accessing a person's DNA for hacker's purposes.

68. Data Breach victims suffer long-term consequences when their Social Security numbers are taken and used by hackers. Even if they know their Social Security numbers are being misused, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of Social Security number misuse.

69. The Social Security Administration has warned that "a new number probably won't solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number

[22] "Victims of Identity Theft, 2018," U.S. Department of Justice (April 2021, NCJ 256085), *available at* https://bjs.ojp.gov/content/pub/pdf/vit18.pdf (last accessed on January 26, 2023).

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

won't guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same."[23]

70. In 2021, there were a record setting 1,862 data breaches, surpassing both 2020's total of 1,108 and the previous record of 1,506 set in 2017.[24]

71. Additionally in 2021, there was a 15.1% increase in cyberattacks and data breaches since 2020. According to a poll, security executives predict an increase in attacks from "social engineering and ransomware" over the next two years, as nation-states and cybercriminals grow more sophisticated. Unfortunately, these preventable causes will largely come from "misconfigurations, human error, poor maintenance, and unknown assets."[25]

72. In light of high-profile data breaches at other industry leading companies, including Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Convergent knew or should have known that its computer network would be targeted by cybercriminals.

73. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so those targets are aware of, can prepare for, and hopefully can ward off a cyberattack.

74. According to an FBI publication, "[r]ansomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to

---

[23] https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed on January 26, 2023).

[24] https://www.cnet.com/tech/services-and-software/record-number-of-data-breaches-reported-in-2021-new-report-says/ (last accessed on January 26, 2023).

[25] https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=176bb6887864 (last accessed on January 26, 2023).

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

operations and the loss of critical information and data."[26] This publication also explains that "[t]he FBI does not support paying a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee you or your organization will get any data back. It also encourages perpetrators to target more victims and offers an incentive for others to get involved in this type of illegal activity." [27]

75. Ransomware attacks, like that the one Defendant experienced,[28] are a well-known threat to companies that maintain Private Information. Companies should treat ransomware attacks as any other data breach incident because ransomware attacks don't just hold networks hostage, "ransomware groups sell stolen data in cybercriminal forums and dark web marketplaces for additional revenue."[29] As cybersecurity expert Emisoft warns, "[a]n absence of evidence of exfiltration should not be construed to be evidence of its absence . . . the initial assumption should be that data may have been exfiltrated."

76. An increasingly prevalent form of ransomware attack is the "encryption+exfiltration" attack in which the attacker encrypts a network and exfiltrates the data contained within.[30]

77. In 2020, over 50% of ransomware attackers exfiltrated data from a network before encrypting it.[31] Once the data is exfiltrated from a network, its confidential nature is destroyed and it should be "assume[d] [the data] will be traded to other threat actors, sold, or held for a

---

[26] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware (last accessed on January 26, 2023).

[27] *Id.*

[28] https://www.hipaajournal.com/ransomware-attacks-announced-by-maternal-family-health-services-and-retreat-behavioral-health/.

[29] *Ransomware: The Data Exfiltration and Double Extortion Trends*, *available at* https://www.cisecurity.org/insights/blog/ransomware-the-data-exfiltration-and-double-extortion-trends

[30] *The chance of data being stolen in a ransomware attack is greater than one in ten*, available at https://blog.emsisoft.com/en/36569/the-chance-of-data-being-stolen-in-a-ransomware-attack-is-greater-than-one-in-ten/.

[31] 2020 Ransomware Marketplace Report, available at https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

second/future extortion attempt."[32] And even where companies pay for the return of data, attackers often leak or sell the data regardless because there is no way to verify copies of the data are destroyed.[33]

78. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

79. Despite the prevalence of public announcements of data breach and data security compromises, despite its own acknowledgments of data security compromises, and despite its own acknowledgment of its duties to keep Private Information confidential and secure, Convergent failed to take appropriate steps to protect the Private Information of Plaintiffs and the proposed Class from being compromised.

80. Convergent failed to abide by its own Privacy Policy.[34]

Convergent Had a Duty to Properly Secure Private Information

81. At all relevant times, Convergent had a duty to Plaintiffs and Class Members to properly secure their Private Information, encrypt and maintain such information using industry standard methods, train its employees, utilize available technology to defend its systems from invasion, act reasonably to prevent foreseeable harm to Plaintiffs and Class Members, and to promptly notify Plaintiffs and Class Members when Convergent became aware that their Private Information was compromised.

82. Convergent had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect the information it

---

[32] *Id.*

[33] *Id.*

[34] https://www.convergentusa.com/outsourcing/page/privacy-policy#q2 (last accessed on January 26, 2023).

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

maintained. Accordingly, Convergent breached its common law, statutory, and other duties owed to Plaintiffs and Class Members.

83. Security standards commonly accepted among businesses that store Private Information using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;

c. Monitoring for suspicious or irregular traffic to servers;

d. Monitoring for suspicious credentials used to access servers;

e. Monitoring for suspicious or irregular activity by known users;

f. Monitoring for suspicious or unknown users;

g. Monitoring for suspicious or irregular server requests;

h. Monitoring for server requests for PII;

i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

84. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[35] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[36]

[35] 17 C.F.R. § 248.201 (2013).
[36] *Id.*

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

85. The ramifications of Convergent's failure to keep consumers' Private Information secure are long lasting and severe. Once Private Information is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims—including Plaintiffs and the Class—may continue for years.

The Value of Personal Identifiable Information

86. The Private Information of consumers remains of high value to criminals, as evidenced by the prices criminals will pay through the dark web for this information. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200.[37]

87. Criminals can also purchase access to entire company's data breaches from $900 to $4,500.[38]

88. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[39]

89. An active and robust legitimate marketplace for Private Information also exists. In 2019, the data brokering industry was worth roughly $200 billion.[40] In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or

---

[37] *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed on January 26, 2023).

[38] *In the Dark*, VPNOverview, 2019, *available at* https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed on January 26, 2023).

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

[40] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Sept. 13, 2022).

app developers.[41,42] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[43]

90. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiff or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

91. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[44]

92. Attempting to change or cancel a stolen Social Security number is difficult if not nearly impossible. An individual cannot obtain a new Social Security number without evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of

---

[41] https://www.latimes.com/business/story/2019-11-05/column-data-brokers.

[42] https://datacoup.com/.

[43] https://digi.me/what-is-digime/.

[44] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed on January 26, 2023).

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

93. Even a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[45]

94. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[46]

95. Private Information can be used to distinguish, identify, or trace an individual's identity, such as their name and Social Security number. This can be accomplished alone, or in combination with other personal or identifying information that is connected or linked to an individual, such as their birthdate, birthplace, and mother's maiden name.[47]

96. Given the nature of this Data Breach, it is foreseeable that the compromised Private Information can be used by hackers and cybercriminals in a variety of devastating ways. Indeed, the cybercriminals who possess Class Members' Private Information can easily obtain Class Members' tax returns or open fraudulent credit card accounts in Class Members' names.

97. The Private Information compromised in this Data Breach is static and difficult, if not impossible, to change (such as Social Security numbers).

---

[45] Brian Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-identity-theft (last accessed on January 26, 2023).

[46] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, Computer World (Feb. 6, 2015), http://www.itworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed on January 26, 2023).

[47] *See* Office of Mgmt. & Budget, OMB Memorandum M-07-16 n. 1 (last accessed on January 26, 2023).

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

98. Moreover, Convergent has offered only a limited subscription for identity theft monitoring and identity theft protection through IDX. Its limitation is inadequate when IDX's victims are likely to face many years of identity theft, and they will be forced to pay for necessary credit monitoring services out of pocket.

99. Furthermore, Convergent's credit monitoring offer and admonition to Plaintiffs and Class Members to be vigilant for identity theft places the burden squarely on Plaintiffs and Class Members, rather than on Convergent, to monitor and report suspicious activities to law enforcement. In other words, Convergent expects Plaintiffs and Class Members to protect themselves from Convergent' s own tortious acts that resulted in the Data Breach. Rather than automatically enrolling Plaintiffs and Class Members in credit monitoring services upon discovery of the breach, Convergent merely sent instructions to Plaintiffs and Class Members about actions they can affirmatively take to protect themselves.

100. These services are wholly inadequate as they fail to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud, and they entirely fail to provide any compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

101. The injuries to Plaintiffs and Class Members were directly and proximately caused by Convergent's failure to implement or maintain adequate data security measures for the victims of its Data Breach.

Convergent Failed to Comply with FTC Guidelines

102. Federal and State governments have established security standards and issued recommendations to mitigate the risk of data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the

importance of reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.[48]

103. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[49] The guidelines note businesses should protect the personal consumer and consumer information that they keep, as well as properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.

104. The FTC emphasizes that early notification to data breach victims reduces injuries: "If you quickly notify people that their personal information has been compromised, they can take steps to reduce the chance that their information will be misused" and "thieves who have stolen names and Social Security numbers can use that information not only to sign up for new accounts in the victim's name, but also to commit tax identity theft. People who are notified early can take steps to limit the damage."[50]

105. The FTC recommends that companies verify that third-party service providers have implemented reasonable security measures.[51]

106. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

---

[48] Federal Trade Commission, *Start With Security*, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last accessed on January 26, 2023).

[49] Federal Trade Commission, *Protecting Personal Information: A Guide for Business, available at*: https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business (last accessed January 26, 2023).

[50] Federal Trade Commission, *Data Breach Response: A Guide for Business*, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business (last accessed January 26, 2023).

[51] Federal Trade Commission, *Start With Security*, supra note 48.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks.

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

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

108. Because Plaintiffs and Class Members entrusted Convergent with their Private Information, Convergent had, and has, a duty to the Plaintiffs and Class Members to keep their Private Information secure.

109. Plaintiffs and the other Class Members reasonably expected that when they entrusted their Private Information to Convergent (or to Convergent's customers), Convergent would safeguard their Private Information.

110. Convergent was at all times fully aware of its obligation to protect the personal and financial data of consumers, including Plaintiffs and members of the Class. Convergent was also aware of the significant repercussions if it failed to do so. Its own Privacy Policies, quoted above, acknowledge this awareness.

111. Convergent's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—including Plaintiffs' and Class Members' first names, last names, addresses, and Social Security numbers, and other highly

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

sensitive and confidential information—constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Plaintiffs and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security

112. Plaintiffs and Class Members reasonably expected that Defendant would provide adequate security protections for their Private Information, and Class Members provided Defendant with sensitive personal information, including their names, addresses, and Social Security numbers.

113. Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain. Plaintiffs and other individuals whose Private Information was entrusted to Convergent understood and expected that, as part of that business relationship, they would receive data security, when in fact Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received data security that was of a lesser value than what they reasonably expected. As such, Plaintiffs and the Class Members suffered pecuniary injury.

114. Cybercriminals intentionally targeted, attacked and exfiltrated the Private Information to exploit it. Thus, Plaintiffs and Class Members are now, and for the rest of their lives will be, at a present and continued risk of identity theft. Plaintiffs have also incurred (and will continue to incur) damages in the form of, inter alia, loss of privacy and costs of engaging adequate credit monitoring and identity theft protection services.

115. The cybercriminals who obtained the Class Members' Private Information may exploit the information they obtained by selling the data in so-called "dark markets" or on the "dark web." Having obtained these names, addresses, Social Security numbers, and other Private Information, cybercriminals can pair the data with other available information to commit a broad range of fraud in a Class Member's name, including but not limited to:

- obtaining employment;

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

- obtaining a loan;
- applying for credit cards or spending money;
- filing false tax returns;
- stealing Social Security and other government benefits; and
- applying for a driver's license, birth certificate, or other public document.

116. In addition, if a Class Member's Social Security number is used to create false identification for someone who commits a crime, the Class Member may become entangled in the criminal justice system, impairing the person's ability to gain employment or obtain a loan.

117. As a direct and/or proximate result of Defendant's wrongful actions and/or inaction and the resulting Data Breach, Plaintiffs and the other Class Members have been deprived of the value of their Private Information, for which there is a well-established national and international market.

118. Furthermore, Private Information has a long shelf-life because it contains different forms of personal information, it can be used in more ways than one, and it typically takes time for an information breach to be detected.

119. Accordingly, Defendant's wrongful actions and/or inaction and the resulting Data Breach have also placed Plaintiffs and the other Class Members at an imminent, immediate, and continuing increased risk of identity theft and identity fraud. Indeed, "[t]he level of risk is growing for anyone whose information is stolen in a data breach." Javelin Strategy & Research, a leading provider of quantitative and qualitative research, notes that "[t]he theft of SSNs places consumers at a substantial risk of fraud."[52] Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have

[52] The Consumer Data Insecurity Report: Examining The Data Breach- Identity Fraud Paradigm In Four Major Metropolitan Areas, *available at* https://www.it.northwestern.edu/bin/docs/TheConsumerDataInsecurityReport_byNCL.pdf (last accessed January 26, 2023).

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' Private Information will do so at a later date or re-sell it.

120. As a result of the Data Breach, Plaintiffs and Class Members have already suffered injuries, and each are at risk of a substantial and imminent risk of future identity theft.

121. As Convergent admits, the "the unauthorized actor deployed certain data extraction tools" on its computer systems and the cybercriminals actually exfiltrated the Private Information that was accessed.[53]

Plaintiffs' Experiences

Plaintiff Guy

122. Plaintiff Guy is a consumer and apparent victim of the Data Breach, having received the Notice Letter from Convergent on or about October 31, 2022.

123. The Notice Letter stated that the extracted information included his "name, contact information, financial account number, and Social Security number" but did not expand on whether additional information was stolen as well.

124. Plaintiff Guy is alarmed by the amount of his Private Information that was stolen or accessed, and even more by the fact that his Social Security number was identified as among the breached data on Convergent's computer system.

125. As a result of the Data Breach, Plaintiff Guy has been receiving a combination of around 20 spam calls and many spam emails per day. Many of the spam emails include adult related material or CBD products. His email spam has increased at least ten times since August 2022, to the point that he now receives up to fifty or so a day. Prior to this time, he was not receiving these spam calls and emails.

[53] *See* Notice Letter, Ex. A.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

126. Plaintiff Guy is concerned that the spam calls and texts are being placed with the intent of obtaining more personal information from him and committing identity theft by way of a social engineering or phishing attack.

127. In response to Convergent's Notice of Data Breach, Plaintiff Guy will be required to spend time dealing with the consequences of the Data Breach, which will continue to include time spent verifying the legitimacy of the Notice of Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. He realizes he will likely have to spend about an hour a week verifying financial accounts to check for fraudulent activities. The time he is forced to spend monitoring and securing his accounts has been lost forever and cannot be recaptured.

128. Immediately after receiving the Notice Letter, Plaintiff Guy spent time discussing his options with a law firm and has started to check his financial accounts in an effort to mitigate the damage that has been caused by Convergent.

129. Plaintiff Guy is very careful about sharing Private Information and has never knowingly transmitted unencrypted Private Information over the internet or any other unsecured source.

130. Plaintiff Guy reasonably believes that his Private Information may have already been sold by the cybercriminals. Had he been notified of Convergent's breach in a timelier manner, he could have attempted to mitigate his injuries.

Plaintiff Tanner

131. Plaintiff Tanner is a consumer and apparent victim of the Data Breach, having received the Notice Letter from Convergent on or about October 31, 2022.

132. The Notice Letter stated that the extracted information included his "name, contact information, financial account number, and Social Security number" but did not expand on whether additional information was stolen as well.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

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

134. Plaintiff Tanner suffered actual injury in the form of damages to and diminution in the value of Plaintiff Tanner's Private Information—a form of intangible property that Plaintiff Tanner entrusted to Defendant—which was compromised in and as a result of the Data Breach.

135. Additionally, Plaintiff Tanner suffered actual injury in the form of fraudulent charges on his financial accounts. Specifically, since the Data Breach, Plaintiff Tanner was made aware of unauthorized charges for Netflix in the amount of approximately $100. Plaintiff, who was unemployed at the time the charges went through, spent several hours attempting to dispute the fraudulent charges with his bank and was forced to borrow money while the charges were being disputed.

136. Plaintiff Tanner suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

137. Plaintiff Tanner has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties and possibly criminals.

138. Plaintiff Tanner has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from future breaches.

Plaintiff Granados

139. Plaintiff Magaly Granados is a consumer and apparent victim of the Data Breach, having received the Notice Letter from Convergent on or about October 31, 2022.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

140. The Notice Letter stated that the extracted information included her "name, contact information, financial account number, and Social Security number" but did not expand on whether additional information was stolen as well.

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

142. Plaintiff Granados suffered actual injury in the form of damages to and diminution in the value of Plaintiff Granados' Private Information—a form of intangible property that Plaintiff Granados entrusted to Defendant—which was compromised in and as a result of the Data Breach.

143. Plaintiff Granados suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

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

145. Plaintiff Granados has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from future breaches.

Plaintiff Lamons

146. Plaintiff Kerry Lamons is a consumer and apparent victim of the Data Breach, having received the Notice Letter from Convergent on or about October 31, 2022r.

147. The Notice Letter indicated that Convergent had known about the Data Breach for over 4 months. The letter stated that the extracted information included her "name, contact information, financial account number, and Social Security number" but did not expand on whether additional information was stolen as well.

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

149. Plaintiff Lamons suffered actual injury in the form of damages to and diminution in the value of Plaintiff Lamons' Private Information—a form of intangible property that Plaintiff Lamons entrusted to Defendant—which was compromised in and as a result of the Data Breach.

150. Plaintiff Lamons suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

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

152. Plaintiff Lamons has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from future breaches.

Plaintiff Rano

153. Plaintiff Tammy Rano is a consumer and apparent victim of the Data Breach, having received the Notice Letter from Convergent on or about October 31, 2022.

154. The Notice Letter indicated that Convergent had known about the Data Breach for over 4 months. The Notice Letter stated that the extracted information included her "name, contact information, financial account number, and Social Security number" but did not expand on whether additional information was stolen as well.

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

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

156. Plaintiff Rano suffered actual injury in the form of damages to and diminution in the value of Plaintiff Rano's Private Information—a form of intangible property that Plaintiff Rano entrusted to Defendant—which was compromised in and as a result of the Data Breach.

157. Plaintiff Rano suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

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

159. Plaintiff Rano has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from future breaches.

Plaintiff Will

160. Plaintiff Vicki Will is a consumer and apparent victim of the Data Breach, having received the Notice Letter from Convergent on or about October 31, 2022.

161. The Notice Letter indicated that Convergent had known about the Data Breach for over 4 months. The Notice Letter stated that the extracted information included her "name, contact information, financial account number, and Social Security number" but did not expand on whether additional information was stolen as well.

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

163. Plaintiff Will suffered actual injury in the form of damages to and diminution in the value of Plaintiff Will's Private Information—a form of intangible property that Plaintiff Will entrusted to Defendant—which was compromised in and as a result of the Data Breach.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

164. Plaintiff Will suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

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

166. Plaintiff Will has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from future breaches.

Plaintiff White

167. Plaintiff Jennifer White is a consumer and apparent victim of the Data Breach, having received the Notice Letter from Convergent on or about October 31, 2022.

168. The Notice Letter indicated that Convergent had known about the Data Breach for over 4 months. The Notice Letter stated that the extracted information included her "name, contact information, financial account number, and Social Security number" but did not expand on whether additional information was stolen as well.

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

170. Plaintiff White suffered actual injury in the form of damages to and diminution in the value of Plaintiff White's Private Information—a form of intangible property that Plaintiff Will entrusted to Defendant—which was compromised in and as a result of the Data Breach.

171. Plaintiff White suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

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

173. Plaintiff White has a continuing interest in ensuring that her Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from future breaches.

Common Injuries

174. All Plaintiffs have suffered present, continued, and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from their stolen Private Information, especially Social Security numbers, being placed in the hands of criminals.

175. All Plaintiffs have a continuing interest in ensuring that their Private Information, which upon information and belief remains backed up and in Convergent's possession, is protected and safeguarded from future breaches.

176. All Plaintiffs have suffered actual injury and damages as a result of the Data Breach. Plaintiffs would not have provided Convergent with their Private Information had Convergent disclosed that it lacked data security practices adequate to safeguard Private Information

177. All Plaintiffs suffered actual injury in the form of damages and diminution in the value of their Private Information—a form of intangible property that they entrusted to Convergent (or its customers).

178. All Plaintiffs have suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and increased concerns for the loss of their privacy, especially their Social Security numbers.

CLASS ACTION ALLEGATIONS

179. Plaintiffs bring this action on behalf of themselves and on behalf of all other persons similarly situated.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

180. Plaintiffs propose the following Class definition, subject to amendment as appropriate:

> All persons whose Private Information was maintained on Defendant Convergent Outsourcing, Inc.'s computer systems and compromised in Convergent's June 2022 Data Breach ("the Class").

181. Plaintiffs also seek to represent the following state subclass defined as:

> All California residents whose Private Information was maintained on Defendant Convergent Outsourcing, Inc.'s computer systems and compromised in Convergent's June 2022 Data Breach (the "California Subclass").

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

183. Plaintiffs hereby reserve the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

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

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

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

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

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

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

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

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

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

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

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

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

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

l. Whether Defendant's acts, inactions, and practices complained of herein violated the state data protection laws invoked below;

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

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

186. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class member, was compromised in the Data Breach.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

187. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating Class actions.

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

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

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

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

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

- Whether Defendant owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;
- Whether Defendant's security measures to protect its data systems were reasonable in light of best practices recommended by data security experts;
- Whether Defendant's failure to institute adequate protective security measures amounted to negligence;
- Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and
- Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

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

CAUSES OF ACTION

FIRST COUNT

Negligence
(On behalf of Plaintiffs and All Class Members)

193. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

194. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of the regular course of its business operations. Plaintiffs and Class Members were entirely dependent on Defendant to use reasonable measures to safeguard their Private Information and were vulnerable to the foreseeable harm described herein should Defendant fail to safeguard their Private Information.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

195. By collecting and storing this data in its computer property, and sharing it, and using it for commercial gain, Defendant assumed a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within its computer property—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of their security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a Data Breach.

196. Defendant owed a duty of care to Plaintiffs and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

197. Defendant had a duty to employ reasonable security measures under Section 5 of the FTC Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

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

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

200. Defendant gathered and stored the Private Information of Plaintiffs and Class Members as part of its business of soliciting its services to its clients and its clients' customers, which solicitations and services affect commerce.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

201. Defendant violated the FTC Act by failing to use reasonable measures to protect the Private Information of Plaintiffs and Class Members and by not complying with applicable industry standards, as described herein.

202. Defendant breached its duties to Plaintiffs and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and/or data security practices to safeguard Plaintiffs' and Class Members' Private Information, and by failing to provide prompt notice without reasonable delay.

203. Defendant's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

204. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

205. Defendant had full knowledge of the sensitivity of the Private Information, the types of harm that Plaintiffs and Class Members could and would suffer if the Private Information was wrongfully disclosed, and the importance of adequate security.

206. Plaintiffs and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiffs and the Class members had no ability to protect their Private Information that was in Defendant's possession.

207. Defendant was in a special relationship with Plaintiffs and Class Members with respect to the hacked information because the aim of Defendant's data security measures was to benefit Plaintiffs and Class Members by ensuring that their personal information would remain protected and secure. Only Defendant was in a position to ensure that its systems were sufficiently secure to protect Plaintiffs' and Class Members' Private Information. The harm to Plaintiffs and Class Members from its exposure was highly foreseeable to Defendant.

208. Defendant owed Plaintiffs and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

obtaining, storing, using, and managing their Private Information, including taking action to reasonably safeguard such data and providing notification to Plaintiffs and the Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

209. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures have also recognized the existence of a specific duty to reasonably safeguard personal information.

210. Defendant had duties to protect and safeguard the Private Information of Plaintiffs and the Class from being vulnerable to compromise by taking common-sense precautions when dealing with sensitive Private Information. Additional duties that Defendant owed Plaintiffs and the Class include:

a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendant' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiffs' and Class members' Private Information was adequately secured from impermissible release, disclosure, and publication;

b. To protect Plaintiffs' and Class Members' Private Information in its possession by using reasonable and adequate security procedures and systems; and

c. To promptly notify Plaintiffs and Class Members of any breach, security incident, unauthorized disclosure, or intrusion that affected or may have affected their Private Information.

211. Only Defendant was in a position to ensure that its systems and protocols were sufficient to protect the Private Information that had been entrusted to them.

212. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and Class Members' Private Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining, securing, safeguarding, protecting, and deleting the Private Information in its possession;

b. Failing to protect the Private Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Private Information;

d. Failing to adequately train its employees to not store unencrypted Private Information in their personal files longer than absolutely necessary for the specific purpose that it was sent or received;

e. Failing to consistently enforce security policies aimed at protecting Plaintiffs' and Class Members' Private Information;

f. Failing to mitigate the harm caused to Plaintiffs and the Class Members;

g. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions; and

h. Failing to promptly notify Plaintiffs and Class Members of the Data Breach that affected their Private Information.

213. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

214. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and Class Members have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

215. Through Defendant's acts and omissions described herein, including but not limited to Defendant's failure to protect the Private Information of Plaintiffs and Class Members from being stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure the Private Information of Plaintiffs and Class Members while it was within Defendant's possession and control.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

216. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiffs and Class Members, Defendant prevented Plaintiffs and Class Members from taking meaningful, proactive steps to securing their Private Information and mitigating damages.

217. As a result of the Data Breach, Plaintiffs and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, responding to the fraudulent use of the Private Information, and closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies.

218. Defendant's wrongful actions, inaction, and omissions constituted (and continue to constitute) common law negligence.

219. The damages Plaintiffs and the Class have suffered (as alleged above) and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

220. Plaintiffs and the Class have suffered injury and are entitled to actual damages in amounts to be proven at trial.

SECOND COUNT

Breach of Implied Contract
(On Behalf of Plaintiffs and All Class Members)

221. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

222. Plaintiffs and Class Members were required to provide their Private Information to Defendant as a condition of receiving other services provided by Defendant.

223. Plaintiffs and Class Members provided their Private Information to Defendant or its third-party agents in exchange for Convergent's services or employment. In exchange for the Private Information, Defendant promised to protect their Private Information from unauthorized disclosure.

224. At all relevant times Defendant promulgated, adopted, and implemented written a Privacy Policy whereby it expressly promised Plaintiffs and Class Members that it would only disclose Private Information under certain circumstances, none of which relate to the Data Breach.

225. On information and belief, Defendant further promised to comply with industry standards and to make sure that Plaintiffs' and Class Members' Private Information would remain protected.

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

227. When Plaintiffs and Class Members provided their Private Information to Defendant as a condition of relationship, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

228. Defendant required Class Members to provide their Private Information as part of Defendant's regular business practices.

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

230. Plaintiffs and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiffs and Class Members would not have entrusted their

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that it adopted reasonable data security measures.

231. Plaintiffs and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

232. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

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

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

235. Plaintiffs and Class Members are also entitled to nominal damages for the breach of implied contract.

236. Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate long term credit monitoring to all Class Members for a period longer than the grossly inadequate one-year currently offered.

THIRD COUNT

Breach of Confidence
(On Behalf of Plaintiffs and All Class Members)

237. Plaintiffs incorporate by reference the foregoing allegations of fact as if fully set forth herein.

238. At all times Defendant collected and maintained Plaintiffs' and the Class Members' Private Information, Defendant was fully aware of the confidential and sensitive nature of the Private Information that Plaintiffs and the Class provided to Defendant.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

239. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and the Class Members' Private Information would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

240. Plaintiffs and Class Members entrusted their Private Information to Defendant with the implicit understanding that Defendant or anyone in Defendant's position would protect and not permit the Private Information to be disseminated to any unauthorized third parties.

241. Plaintiffs and Class Members also entrusted their Private Information to Defendant with the implicit understanding that Defendant or anyone in Defendant's position would take precautions to protect that Private Information from unauthorized disclosure.

242. Defendant voluntarily received in confidence Plaintiffs' and the Class Members' Private Information with the understanding that Private Information would not be disclosed or disseminated to the public or any unauthorized third parties.

243. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and the Class Members' Private Information was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and the Class Members' confidence, and without their express permission.

244. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

245. But for Defendant's disclosure of Plaintiffs' and the Class Members' Private Information in violation of Defendant's assumption of a duty of confidence, their Private Information would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and the Class Members' Private Information as well as the resulting damages.

246. The injury and harm Plaintiffs and Class Members suffered were the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and the Class Members'

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

Private Information. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and the Class Members' Private Information was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and the Class Members' Private Information.

247. As a direct and proximate result of Defendant's breach of its confidence with Plaintiffs and the Class, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual present and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of current and former patients and their beneficiaries and dependents; and (viii) present and future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Class.

248. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

FOURTH COUNT

Invasion of Privacy
(On Behalf of Plaintiffs and All Class Members)

249. Plaintiffs incorporate by reference the foregoing allegations of fact as if fully set forth herein.

250. Plaintiffs and Class Members reasonably expected that the sensitive Private Information entrusted to Defendant would be kept private and secure and would not be disclosed to any unauthorized third party or for any improper purpose.

251. Defendant unlawfully invaded the privacy rights of Plaintiffs and Class Members by:

a. Failing to adequately secure their sensitive Private Information from disclosure to unauthorized third parties or for improper purposes;

b. Enabling the disclosure of personal and sensitive facts and information about them in a manner highly offensive to a reasonable person; and

c. Enabling the disclosure of personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

252. A reasonable person would find it highly offensive that Defendant, having collected Plaintiffs' and Class Members' sensitive Private Information, failed to protect such Private Information from unauthorized disclosure to third parties.

253. In failing to adequately protect Plaintiffs' and Class Members' sensitive personal information, Defendant acted in reckless disregard of their privacy rights. Defendant knew or should have known that its ineffective security measures, and the foreseeable consequences thereof, are highly offensive to a reasonable person in Plaintiffs' and Class Members' position.

254. Defendant violated Plaintiffs' and Class Members' right to privacy under the common law.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

255. Defendant's unlawful invasions of privacy damaged Plaintiffs and Class Members. As a direct and proximate result of Defendant's unlawful invasion of privacy, Plaintiffs and Class Members suffered significant anxiety and distress, and their reasonable expectations of privacy were frustrated and defeated. Plaintiffs and the Class seek actual and nominal damages for these invasions of privacy.

FIFTH COUNT

Unjust Enrichment
(On Behalf of Plaintiffs and All Class Members)

256. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

257. Plaintiffs bring this Count in the alternative their breach of contract claim.

258. Plaintiffs and Class Members conferred a monetary benefit on Defendant in the form of the provision of their Private Information and Defendant would be unable to engage in its regular course of business without that Private Information.

259. Defendant appreciated that a monetary benefit was being conferred upon it by Plaintiffs and Class Members and accepted that monetary benefit.

260. However, acceptance of the benefit under the facts and circumstances outlined above make it inequitable for Defendant to retain that benefit without payment of the value thereof. Specifically, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Personal Information. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own profits at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite data security.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

261. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiffs and Class Members, because Defendant failed to implement appropriate data management and security measures.

262. Defendant acquired the Private Information through inequitable means in that it failed to disclose the inadequate security practices previously alleged.

263. If Plaintiffs and Class Members had known that Defendant had not secured their PII, they would not have agreed to provide their PII to Defendant.

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

265. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have suffered or will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in their continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

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

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

267. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class Members, proceeds that they unjustly received from them.

SIXTH COUNT

Declaratory Judgment
(On Behalf of Plaintiffs and All Class Members)

268. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

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

270. An actual controversy has arisen in the wake of the Convergent Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' Personal Information and whether Convergent is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further data breaches that compromise their Private Information.

271. Plaintiffs allege that Convergent's data security measures remain inadequate. Plaintiffs will continue to suffer injury because of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

272. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Convergent continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various states' statutes;

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

b. Convergent continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

273. The Court also should issue corresponding prospective injunctive relief requiring Convergent to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

274. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Convergent. The risk of another such breach is real, immediate, and substantial. If another breach at Convergent occurs, Plaintiffs and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

275. The hardship to Plaintiffs and class members if an injunction does not issue exceeds the hardship to Convergent if an injunction is issued. Among other things, if another massive data breach occurs at Convergent, Plaintiffs and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Convergent of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Convergent has a pre-existing legal obligation to employ such measures.

276. Issuance of the requested injunction will not do a disservice to the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Convergent, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised.

SEVENTH COUNT

Violation of the Washington Consumer Protection Act
RCW 19.86.010, *et seq.*,
(On Behalf of Plaintiffs and All Class Members)

277. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

278. The Washington State Consumer Protection Act, RCW 19.86.020 (the "CPA") prohibits any "unfair or deceptive acts or practices" in the conduct of any trade or commerce as those terms are described by the CPA and relevant case law.

279. Defendant is a "person" as described in RWC 19.86.010(1).

280. Defendant engages in "trade" and "commerce" as described in RWC 19.86.010(2) in that they engage in the sale of services and commerce directly and indirectly affecting the people of the State of Washington.

281. By virtue of the above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach, Defendant engaged in unlawful, unfair and fraudulent practices within the meaning, and in violation of, the CPA, in that Defendant's practices were injurious to the public interest because they injured other persons, had the capacity to injure other persons, and have the capacity to injure other persons.

282. Defendant's failure to safeguard the Personal Information exposed in the Data Breach constitutes an unfair act that offends public policy.

283. Defendant's failure to safeguard the Personal Information compromised in the Data Breach caused substantial injury to Plaintiffs and Class Members. Defendant's failure is not outweighed by any countervailing benefits to consumers or competitors, and it was not reasonably avoidable by consumers.

284. Defendant's failure to safeguard the Personal Information disclosed in the Data Breach, and its failure to provide timely and complete notice of that Data Breach to the victims, is unfair because these acts and practices are immoral, unethical, oppressive, and/or unscrupulous.

285. In the course of conducting their business, Defendant committed "unfair or deceptive acts or practices" by, inter alia, knowingly failing to design, adopt, implement, control,

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' Private Information, and violating the common law alleged herein in the process. Plaintiffs and Class Members reserve the right to allege other violations of law by Defendant constituting other unlawful business acts or practices. As described above, Defendant's wrongful actions, inaction, omissions, and want of ordinary care are ongoing and continue to this date.

286. Defendant also violated the CPA by failing to timely notify, and by concealing from Plaintiffs and Class Members, information regarding the unauthorized release and disclosure of their Private Information. If Plaintiffs and Class Members had been notified in an appropriate fashion, and had the information not been hidden from them, they could have taken precautions to safeguard and protect their Private Information and identities.

287. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, misrepresentations, practices, and non-disclosures also constitute "unfair or deceptive acts or practices" in violation of the CPA in that Defendant's wrongful conduct is substantially injurious to other persons, had the capacity to injure other persons, and has the capacity to injure other persons.

288. The gravity of Defendant's wrongful conduct outweighs any alleged benefits attributable to such conduct. There were reasonably available alternatives to further Defendant's legitimate business interests other than engaging in the above-described wrongful conduct.

289. Defendant's unfair or deceptive acts or practices occurred in its trade or business and have and injured and are capable of injuring a substantial portion of the public. Defendant's general course of conduct as alleged herein is injurious to the public interest, and the acts complained of herein are ongoing and/or have a substantial likelihood of being repeated.

290. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

Data Breach and their violations of the CPA, Plaintiffs and Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia, (1) an imminent, immediate and the continuing increased risk of identity theft, identity fraud—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (2) invasion of privacy; (3) breach of the confidentiality of their Private Information; (5) deprivation of the value of their Private Information, for which there is a well-established national and international market; and/or (6) the financial and temporal cost of monitoring credit, monitoring financial accounts, and mitigating damages.

291. Unless restrained and enjoined, Defendant will continue to engage in the above-described wrongful conduct and more data breaches will occur. Plaintiffs, therefore, on behalf of themselves and the Class, seek restitution and an injunction prohibiting Defendant from continuing such wrongful conduct, and requiring Defendant to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures protocols, and software and hardware systems to safeguard and protect the Private Information entrusted to it.

292. Plaintiffs, on behalf of themselves and Class Members, also seek to recover actual damages sustained by each Class Member together with the costs of the suit, including reasonable attorney fees. In addition, Plaintiffs, on behalf of themselves and Class Members, request that this Court use its discretion, pursuant to RCW 19.86.090, to increase the damages award for each Class Member by three times the actual damages sustained not to exceed $25,000.00 per Class Member.

EIGHTH COUNT

Violation of the Washington Data Breach Disclosure Law (On Behalf of Plaintiffs and All Class Members)

293. Plaintiffs re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

294. Under RCW § 19.255.010(2), "[a]ny person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person."

295. Here, the Data Breach led to "unauthorized acquisition of computerized data that compromise[d] the security, confidentiality, [and] integrity of personal information maintained by" Defendant, leading to a "breach of the security of [Defendant's] systems," as defined by RCW § 19.255.010.

296. Defendant failed to disclose that the Private Information-of Plaintiffs and Class Members-that had been compromised "immediately" upon discovery, and thus unreasonably delayed informing Plaintiffs and the proposed Class about the Data Breach. Instead, Defendant waited over four months to begin notifying the Class.

NINTH COUNT

Violation of the California Consumer Privacy Act ("CCPA")
Cal. Civ. Code § 1798, *et seq.*
(On Behalf of Plaintiffs Lamons and White and California Subclass Members)

297. Plaintiffs Lamons and White re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

298. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:

(A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

299. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

300. Plaintiffs and California subclass members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

301. The personal information of Plaintiffs and the California subclass at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted:(i) Social security number;(ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual;(iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information;(v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

302. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the California subclass's personal information and that the risk of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs and the California subclass. Specifically, Defendant subjected Plaintiff's and the California subclass's nonencrypted and nonredacted Private Information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

303. As a direct and proximate result of Defendant' violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and Class Members' personal information included exfiltration, theft, or disclosure through Defendant' servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

304. As a direct and proximate result of Defendant' acts, Plaintiffs and the California subclass were injured and lost money or property, including but not limited to the loss of Plaintiffs' and the subclass's legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

305. Section 1798.150(b) specifically provides that "[n]o[prefiling]notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiffs and the California subclass by way of this complaint seek actual pecuniary damages suffered as a result of Defendant' violations described herein. Plaintiffs has issued and/or will issue a notice of these alleged violations pursuant to § 1798.150(b) and intend to amend this complaint to seek statutory damages and injunctive relief upon expiration of the 30-day cure period pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b).

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

TENTH COUNT

California Unfair Competition Law ("UCL")
Cal. Bus. & Prof. Code § 17200, *et seq*.
(On Behalf of Plaintiffs Lamons and White and California Subclass Members)

306. Plaintiffs Lamons and White re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

307. Defendant is a "person" as defined by Cal. Bus. & Prof. Code § 17201.

308. Defendant violated Cal. Bus. & Prof. Code § 17200 et seq. ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

309. Defendant' "unfair" acts and practices include:

a. Defendant failed to implement and maintain reasonable security measures to protect Plaintiff's and California subclass members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Defendant data breach. Defendant failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. Defendant' failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 et seq.), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. Defendant' failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above,

that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of Defendant' inadequate security, consumers could not have reasonably avoided the harms that Defendant caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

310. Defendant have engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, et seq., the FTC Act, 15 U.S.C.§ 45, and California common law.

311. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California subclass members' personal information, which was a direct and proximate cause of the Defendant data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Defendant's data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150,

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

which was a direct and proximate cause of the Defendant's data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and California subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California subclass members' personal information, including duties imposed by the FTC Act, 15U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and California subclass members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, et seq., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.

312. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

313. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California subclass members were injured and lost money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, monetary damages from fraud and identity theft, time and expenses

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

314. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

315. Plaintiffs and Class Members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

316. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiffs and class members.

317. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and California subclass members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

318. Plaintiffs and California subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

ELEVENTH COUNT

California Invasion of Privacy
Cal. Const. Art. 1, § 1
(On Behalf of Plaintiffs Lamons and White and California Subclass Members)

319. Plaintiffs Lamons and White re-allege and incorporate by reference the paragraphs above as if fully set forth herein.

320. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

321. The right to privacy in California's constitution creates a private right of action against private and government entities.

322. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

323. Defendant violated Plaintiffs' and Class Members' constitutional right to privacy by collecting, storing, and disclosing their personal information in which they had a legally protected privacy interest, and for which they had a reasonable expectation of privacy, in a manner that was highly offensive to Plaintiffs and Class Members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

324. Defendant has intruded upon Plaintiffs' and class members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

325. Defendant has intruded upon Plaintiffs' and class members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

326. Plaintiffs and Class Members had a reasonable expectation of privacy in that: (i) Defendant's invasion of privacy occurred as a result of Defendant's security practices including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiffs and class members did not consent or otherwise authorize Defendant to disclosure their personal information; and (iii) Plaintiffs and class members could not reasonably expect Defendant would commit acts in violation of laws protecting privacy.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

327. As a result of Defendants' actions, Plaintiffs and Class Members have been damaged as a direct and proximate result of Defendant's invasion of their privacy and are entitled to just compensation.

328. Plaintiffs and Class Members suffered actual and concrete injury as a result of Defendant's violations of their privacy interests. Plaintiffs and Class Members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

329. Plaintiffs and Class Members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiffs and Class Members for the harm to their privacy interests as well as disgorgement of profits made by Defendant as a result of its intrusions upon Plaintiff's and Class Members' privacy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiffs and their counsel to represent the Class and Subclass;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures of its Data Breach to Plaintiffs and Class Members;

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

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

E. For declaratory relief as requested;

F. Ordering Defendant to pay for lifetime credit monitoring services for Plaintiffs and the Class;

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

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

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

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

K. Such other and further relief as this Court may deem just and proper.

JURY DEMAND

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

DATED this 10th day of February 2023.

MASON LLP

By: *s/Gary E. Mason*

Gary E. Mason*
Danielle L. Perry*
Lisa A. White*
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015
Telephone: 202.429.2290
gmason@masonllp.com
dperry@masonllp.com
lwhite@masonllp.com

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class

MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC

By: *s/Gary M. Klinger*
Gary M. Klinger**
227 W. Monroe Street, Suite 2100
Chicago, IL 60606
Tel.: (866) 252-0878
Email: gklinger@milberg.com

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class

MORGAN & MORGAN COMPLEX LITIGATION GROUP

By: s/*Jean S. Martin*
Jean S. Martin*
Email: jeanmartin@ForThePeople.com
Francesca Kester**
Email: fkester@ForThePeople.com
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: (813) 559-4908

Interim Co-Lead Counsel for Plaintiffs and the Proposed Class & Co-Lead Whip

TOUSLEY BRAIN STEPHENS PLLC

By: *s/Cecily C. Jordan*
Kim D. Stephens, P.S., WSBA #11984
Email: kstephens@tousley.com
Jason T. Dennett, WSBA #30686
Email: jdennett@tousley.com
Cecily C. Jordan, WSBA #50061
Email: cjordan@tousley.com
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101-3147
Tel: 206.682.5600
Fax: 206.682.2992

Local Liaison Counsel for Plaintiffs and the Proposed Class

*by pro hac vice admission

**application for pro hac vice admission to be filed.

MASON LLP
5335 Wisconsin Avenue, NW, Suite 640
Washington, DC 20015 ~ (202) 429-2290

EXHIBIT A

P.O Box 989728
West Sacramento, CA 95798-9728

[redacted]

To Enroll, Please Call:
1-833-814-1691
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: [redacted]

Leo P Guy
[redacted]
Derry, NH
[redacted]

October 26, 2022

NOTICE OF DATA BREACH

Dear Leo Guy:

Convergent Outsourcing, Inc. ("Convergent") is sending this letter as part of our commitment to privacy. Convergent performs debt collection services and, during the course of performing those services, receives personal information. We are contacting you regarding a security incident at Convergent which may have involved some of your personal information.[1] We want you to understand what happened, what we are doing about it, the steps you can take to protect yourself, and how we can help you.

What Happened.

On June 17, 2022, we became aware of an interruption to certain services performed by Convergent affecting certain computer systems. We immediately began taking steps to secure our systems and launched an investigation to better understand the nature of the service interruption. We immediately took action to secure our systems, isolated any impacted servers against additional spread and severed the unauthorized actor's access to our network and servers. We, with the assistance of third party experts, also expanded our investigation to search for and review any personal information on our systems that could have been accessed.

We discovered that an external actor gained unauthorized access to our systems and deployed a ransomware malware. The investigation also revealed that the unauthorized actor deployed certain data extraction tools on one storage drive that is used to save and share files internally.

What Information Was Involved.

Please note that we are providing this information in an abundance of caution, as the thorough investigation could not confirm your personal information was *actually* viewed by the unauthorized actor.

However, our investigation revealed the following personal information may have been involved in the unauthorized actor's access of the internal drive referenced above: name, contact information, financial account number, and social security number.

What We Are Doing.

Convergent takes the confidentiality, privacy, and security of information in our care seriously. When we discovered the

---

[1] Note, the security incident also impacted the business operations of Convergent's affiliate, Account Control Technology, Inc. ("ACT"). To the best of our knowledge, per our investigation, you are receiving this letter because your information was found in certain information held in connection with Convergent's operations.