#1

COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss. SUPERIOR COURT DEPARTMENT

JORGE CIFUENTES, on behalf of himself individually and on behalf of all others similarly situated,

Plaintiff,

v.

CREATIVE SERVICES, INC.,

Defendant.

Case No. 2273CV00179A

BRISTOL SS SUPERIOR COURT
FILED

MAR - 3 2022

MARC J SANTOS, ESQ.
CLERK/MAGISTRATE

CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff Jorge Cifuentes ("Plaintiff" or "Cifuentes"), individually and on behalf of all others similarly situated ("Class Members"), brings this action against Defendant Creative Services, Inc. ("Creative Services" or "Defendant"), a Massachusetts corporation, to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

NATURE OF THE ACTION

1. Defendant Creative Services is a Massachusetts corporation that provides background check services for employment and licensing purposes.

2. This class action arises out of the recent targeted cyberattack and data breach ("Data Breach") on Creative Services' network that resulted in the unauthorized and unlawful access to and compromise of sensitive data. As a result of the Data Breach, Plaintiff and over 164,000 Class

Members[1] 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. Plaintiff and Class Members are currently and will remain at an increased risk for financial and identity fraud.

3. The information that was accessed and compromised in the Data Breach includes, but may not be limited, to the following: full names, dates of birth, Social Security Numbers, and driver's license numbers ("PII").[2]

4. Plaintiff and Class Members entrusted potential employers and others utilizing Defendant's services with their PII as a condition to receiving employment or other services. Plaintiff and Class Members provided their PII with the reasonable expectation that these potential employers and others utilizing Defendant's services would comply with industry standards to protect their PII from unauthorized criminal access. At all times, Plaintiff and Class Members expected that the entrusted PII would remain private with the exception of authorized disclosures.

5. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant's conduct in breaching these duties amounts to negligence and/or recklessness and violates federal and state statutes.

6. Plaintiff brings this class action lawsuit on behalf of himself and those similarly situated to address Defendant's failure to provide: (1) adequate data security practices and policies to safeguard Plaintiff's and Class Members' PII; (2) timely notice to Plaintiff and other Class

---

[1] https://apps.web.maine.gov/online/aeviewer/ME/40/deb00156-358b-4bf5-80e1-cf0d189e9d3c.shtml (last visited March 1, 2022).
[2] *Id.*

Members that their information had been compromised in the Data Breach; (3) adequate notice detailing the specific type of information that was accessed and compromised; (4) compensation for the out of pocket damages and loss of value of time; (5) protection against financial identity fraud; and (6) protection against the future compromise of the PII that remains in Defendant's possession and control.

7. Defendant maintained the PII in a reckless manner. In particular, the PII was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks and in a manner that fell well below industry cyber security standards and practices.

8. Companies that provide background and employment screening are a common target for cyber-attacks like the attack experienced by Defendant. Upon information and belief, the mechanism of the cyberattack and the potential for improper disclosure of Plaintiff's and Class Members' PII in the event of a cyberattack are a known risk to Defendant. Defendant, therefore, was on notice that failing to design, test, and maintain its network and data security policies in a manner that aligned with industry standards would leave Plaintiff's and Class Members' PII vulnerable and at an increased risk for improper disclosure and theft.

9. Armed with the PII accessed in the Data Breach, data thieves can commit a variety of crimes including, but not limit to, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' names and PII to obtain medical services, using Class Members' PII to target other phishing and hacking intrusions, using Class Members' information to obtain government benefits, filing fraudulent tax returns 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.

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

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

12. By his Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PII was accessed during the Data Breach.

13. Plaintiff seeks remedies including, but not limited to, compensatory damages, punitive damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, adequate credit and identity theft monitoring services, and identity theft restoration services funded by Defendant. Plaintiff also seeks an adequate notice regarding the type of financial information improperly disclosed.

14. Accordingly, Plaintiff brings this action against Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) negligence *per se*, (iii) breach of implied contract; and (iv) unjust enrichment.

JURISDICTION AND VENUE

15. This Court has jurisdiction over the subject matter of this action by virtue of G.L. c. 212, § 4.

16. This Court has personal jurisdiction over Creative Services under G.L. c. 223A, § 3, including because Creative Services has engaged in business with Massachusetts entities, and

because Creative Services' actions and inactions have affected Massachusetts residents.

17. Venue is proper in this Court, as a substantial part of the events giving rise to the claims emanated from activities within this County, and Creative Services conducts substantial business in this County.

THE PARTIES

18. Plaintiff Cifuentes is a natural person, a resident, and a citizen of the State of Virginia. Plaintiff Cifuentes has no intention of moving to a different state in the immediate future. Plaintiff Cifuentes is acting on his own behalf and on behalf of others similarly situated. Defendant obtained and continues to maintain Plaintiff Cifuentes's PII and owed him statutory, common law, and contractual duties and obligations to protect that PII from unauthorized access and disclosure. Plaintiff Cifuentes would not have entrusted his PII to any entity had he known that Defendant would fail to maintain adequate data security. Plaintiff Cifuentes's PII was compromised and disclosed as a result of Defendant's inadequate data security, which proximately caused the Data Breach.

19. Defendant Creative Services provides employment screening and background checks for the corporate, government, cannabis, and higher education sectors and is headquartered in Massachusetts.[3]

20. Defendant Creative Services claims it offers "global, full-service employment screening and security consulting firm, serving corporate, nuclear and government market sectors . . . CSI provides screening solutions that reduce client risk at all stages of the employment cycle. CSI's capabilities span from pre-hire options, such as assessment testing and applicant tracking,

[3] https://www.creativeservices.com/about

to traditional background screening services, drug testing, Electronic I-9 and E-Verify, and extend to post-hire solutions including periodic reinvestigations and annual checks."[4]

21. Defendant Creative Services claims it "is an expert in handling and protecting sensitive information. As an industry leader in employment screening, CSI is provided with, and provides to others, personally identifiable and other information . . . CSI considers privacy and information security among our highest priorities. All data is collected, stored and used in compliance with federal, state, and international laws regarding background screening and privacy."[5]

22. Upon information and belief, in the ordinary course of rendering employment screening services, Creative Services requires individuals to provide sensitive personal and PII, such as:

- name,
- date of birth,
- Social Security number, and,
- driver's license number.

23. As a condition of conducting employment screening or background checks, Creative Services requires individuals entrust it with PII. As part of its services, Defendant expressly or impliedly promised individuals that it would provide adequate data security to protect the PII from unlawful disclosure. Defendant's partners relied on Defendant to implement and follow adequate data security policies and protocols, to keep its customers and patient's PII

[4] *Id.*
[5] https://www.creativeservices.com/about/resources/privacy-policy

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

24. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

THE CYBERATTACK AND DATA BREACH

25. On November 26, 2021, Creative Services discovered an unauthorized party copied and potentially removed files from its systems.[6]

26. On January 25, 2022, Creative Services identified a final list of impacted PII, and on February 23, 2022, sent notifications by mail to impacted individuals.[7]

27. Creative Services launched a third-party investigation and determined certain files had been copied from its system.[8]

28. Through the investigation, Defendant "undertook a comprehensive process to identify what information was potentially contained within the impacted files, and to whom that information belonged."[9]

29. While Creative Services stated the Data Breach occurred on November 26, 2021, Creative Services did not begin notifying victims until February 23, 2022 – nearly three months after discovering the Data Breach.[10]

30. As a result of the Data Breach, Plaintiff's and Class Members' PII was accessed, exfiltrated, stolen, and likely placed on the Dark Web.

---

[6] https://apps.web.maine.gov/online/aeviewer/ME/40/deb00156-358b-4bf5-80e1-cf0d189e9d3c.shtml
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] *Id.*

31. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches on companies in the same or similar industry preceding the date of the breach.

32. In light of recent high profile data breaches at other similar companies, Defendant Creative Services knew or should have known that its electronic records and PII maintained would be targeted by cybercriminals and ransomware attack groups.

33. Indeed, cyberattacks on companies like Defendant's have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack.[11]

34. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

35. Furthermore, the PII that was exposed and exfiltrated in the Data Breach was unencrypted. California law requires companies to notify California residents "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person" due to a "data breach of the security of the system[.] Cal. Civ Code § 1798.82(a)(1). Defendant notified the California Attorney General of the Data Breach on or about February 23, 2022, evidencing that the data exposed in the Data Breach was unencrypted.[12]

36. The notice of data breach letter Creative Services issued to Plaintiff, see attached **Exhibit A**, and similarly situated Class Members as a result of the Data Breach indicated that is

[11] *FBI, Secret Service Warn of Targeted*, Law360 (Nov. 18, 2019), https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware (last visited June 23, 2021).
[12] *See* https://oag.ca.gov/ecrime/databreach/reports/sb24-551180 (last visited Mar. 2, 2022).

"working to implement enhanced security measures."[13] This shows that the unauthorized actor gained access to Creative Services' system because its security measures at the time of the Data Breach were insufficient this causing and/or materially contributed to the occurrence of the Data Breach.

Defendant Fails to Comply with FTC Guidelines

34. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

35. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand its network's vulnerabilities; and implement policies to correct any security problems.[14] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[15]

36. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords

---

[13] https://oag.ca.gov/system/files/Creative%20Services%2C%20Inc.%20-%20Sample%20Notice.pdf (last visited on Mar. 3, 2022).
[14] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016). Available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2022).
[15] *Id.*

to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

37. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the 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.

38. Defendant failed to properly implement basic data security practices.

39. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

40. Defendant was at all times fully aware of its obligation to protect the PII of its customers and patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

41. As shown above, experts studying cyber security routinely identify background check and security consultants and their customers as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

42. Several best practices have been identified that at a minimum should be implemented by service provider like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-

malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

43. Other best cybersecurity practices that are standard in the investigation industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

44. Upon information and belief, Defendant failed to meet some or all of these minimum industry standards : the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

45. These foregoing frameworks are existing, effective and applicable industry standards in the background investigation industry, and Defendant, upon information and belief, failed to comply with some or all of these accepted standards, thereby opening the door to the cyber incident and causing the Data Breach.

DEFENDANT'S BREACH

46. Upon information and belief, Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' PII;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to train its employees in the proper handling of emails containing PII and maintain adequate email security practices;

e. Failing to ensure the confidentiality and integrity of electronic PHI it created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

g. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

h. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

i. Failing to adhere to industry standards for cybersecurity as discussed above; and,

j. Otherwise breached its duties and obligations to protect Plaintiff's and Class Members' PII.

47. Defendant negligently and unlawfully failed to safeguard Plaintiff and Class Members' PII by allowing cyberthieves to access Creative Services' computer network and

systems which contained unsecured and unencrypted PII. Creative Services had to implement new cybersecurity measures to attempt patch the security deficiencies that caused the unauthorized actor to gain access to Creative Services' system and exfiltrate Plaintiff's and Class Members' PII.

48. Because Plaintiff's and Class Members' PII was exfiltrated and stolen during the Data Breach, they now face the present and increased risk of fraud and identity theft.

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

49. Cyberattacks and data breaches occurring at companies like Defendant Creative Services are especially problematic because they can negatively impact the overall daily lives of individuals affected by the attack.

50. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[16]

51. That is because any victim of a data breach is exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such

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

as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

52. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[17]

53. Identity thieves use stolen personal information such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

54. Identity thieves can also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

55. Moreover, theft of PII is also gravely serious. PII is an extremely valuable property

[17] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2022).

right.[18]

56. Its value is axiomatic, considering the value of "big data" in corporate America and the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PII has considerable market value.

57. It must also be noted there may be a substantial time lag – measured in years -- between when harm occurs and when it is discovered, and also between when PII and/or financial information is stolen and when it is used.

58. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> *See* GAO Report, at p. 29.

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

60. There is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and Class Members are at an increased risk of fraud and identity theft for many years into the future.

61. Thus, Plaintiff and Class Members must vigilantly monitor their financial and personal accounts for many years to come.

---

[18] *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).

62. PII can sell for as much as $363 per record according to the Infosec Institute.[19] PII is particularly valuable because criminals can use it to target victims with frauds and scams. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

63. For example, the Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines.[20] Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security Numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity.[21] Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

64. Moreover, it is not an easy task to change or cancel a stolen Social Security number.

65. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[22]

66. This data, as one would expect, demands a much higher price on the black market.

---

[19] *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/.
[20] *Identity Theft and Your Social Security Number*, Social Security Administration (2018) at 1. Available at https://www.ssa.gov/pubs/EN-05-10064.pdf (Jan. 19, 2022).
[21] *Id* at 4.
[22] 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.

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."[23]

67. Because of the value of its collected and of stored data, the investigations industry has experienced disproportionally higher numbers of data theft events than other industries.

68. For this reason, Defendant knew or should have known about these dangers and strengthened its data and network systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet Creative Services failed to properly prepare for that risk.

Plaintiff's and Class Members' Damages

69. To date, Defendant has done nothing to provide Plaintiff and the Class Members with relief for the damages they have suffered as a result of the Data Breach.

70. Defendant has merely offered Plaintiff and Class Members complimentary fraud and identity monitoring services for up to twelve (12) months, but this does not compensate them for damages incurred and time spent dealing with the Data Breach.

71. Plaintiff and Class Members have been damaged by the compromise of their PII in the Data Breach.

72. Plaintiff's and Class Members' PII was all compromised in the Data Breach and is now in the hands of the cybercriminals who accessed Defendant's computer systems.

[23] 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.

73. Since being notified of the Data Breach, Plaintiff Cifuentes has spent time dealing with the impact of the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation.

74. Upon information and belief, Plaintiff believes his PII was leaked and published online.

75. Due to the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. This includes changing passwords, and monitoring his depository and credit accounts for fraudulent activity.

76. Plaintiff also intends to implement a credit freeze. Apart from the time it will take to implement the credit freeze, the credit freeze itself will cause Plaintiff additional lost time and inconvenience. The letter Plaintiff received from Defendant even acknowledges that credit freezes "may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit."

77. Plaintiff's PII was compromised as a direct and proximate result of the Data Breach.

78. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at a present, imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

79. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

80. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans, bank accounts, and credit cards opened in their names, medical services billed in their

names, tax return fraud, utility bills opened in their names, credit card fraud, and other similar identity theft.

81. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their PII as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

82. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

83. Plaintiff and Class Members also suffered a loss of value of their PII when it was acquired by cyber thieves in the Data Breach. Numerous courts have recognized the propriety of loss of value damages in related cases.

84. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

85. Moreover, Plaintiff and Class Members have an interest in ensuring that their PII, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing PII is not accessible online and that access to such data is password protected.

86. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered a loss of privacy, and are at an increased risk of future harm.

Plaintiff Cifuentes's Experience

87. Plaintiff Cifuentes provided his personal information to Defendant Creative Services in conjunction with a background investigation conducted by Defendant on behalf of a client, Edgerock Technologies, LLC ("Edgerock").

88. As part of his background investigation, Plaintiff entrusted his PII, and other confidential information such as name, address, Social Security number, phone number, and other PII with the reasonable expectation and understanding that Edgerock and Defendant Creative Services would take at a minimum industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify him of any data security incidents related to him. Plaintiff would not have submitted this information to Edgerock had he known that Creative Services would not take reasonable steps to safeguard his PII.

89. On or about February 23, 2022, months after Creative Services learned of the data

breach, Plaintiff Cifuentes received a letter from Creative Services notifying him that his PII had been improperly accessed and copied by unauthorized third parties. The notice indicated that Plaintiff Cifuentes's PII was compromised as a result of the Data Breach.[24]

90. As a result of the Data Breach, Plaintiff Cifuentes has or will make reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

91. Plaintiff Cifuentes suffered actual injury from having his PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PII, a form of property that Creative Services obtained from Plaintiff Cifuentes ; (b) violation of his privacy rights; (c) the theft of his PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

92. As a result of the Data Breach, Plaintiff Cifuentes is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

93. As a result of the Data Breach, Plaintiff Cifuentes anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Cifuentes will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come.

CLASS ACTION ALLEGATIONS

94. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated ("the Class").

[24] Ex. A. "Notice of Data Incident" Letter addressed to Plaintiff Cifuentes, dated February 23, 2022.

95. Plaintiff proposes the following Class definitions, subject to amendment as appropriate:

> **All persons Creative Services, Inc. identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "Class").**

96. Excluded from the Class are Defendant's officers, directors, and employees; 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.

97. Plaintiff reserves the right to amend or modify the Class definition as this case progresses.

98. 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 Plaintiff at this time, based on information and belief, the Class consists of over 164,000 individuals whose PII was compromised and exfiltrated as a result of Creative Services' Data Breach.

99. 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 Plaintiff and Class Members' PII;

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;

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 PII;

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

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

h. Whether Defendant should have discovered the Data Breach sooner;

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

j. Whether Defendant's conduct was negligent;

k. Whether Plaintiff and Class Members breached an implied contract between Defendant and Plaintiff's and Class Members' potential employers;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiff and Class Members;

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

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

100. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's information, like that of every other Class Member, was compromised in the Data Breach.

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

102. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all the Plaintiff and Class Members' data was stored on the same computer system 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.

103. 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.

104. 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.

CAUSES OF ACTION

FIRST COUNT
Negligence
(On Behalf of Plaintiff and the Class)

105. Plaintiff re-alleges and incorporates by reference all other paragraphs in the Complaint as if fully set forth herein.

106. Defendant and its customers required prospective employees, including Plaintiff and Class Members, to submit non-public PII in the ordinary course of rendering background checks and other investigative services.

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

108. Defendant owed a duty of care to Plaintiff 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 PII.

109. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and its customers, which is recognized by state and federal laws and regulations, as well as common law. Defendant was in a superior position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

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

111. 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 PII.

112. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PII. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' PII;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to ensure that its networks and systems had plans in place to maintain reasonable data security safeguards;

d. Failing to have in place mitigation policies and procedures;

e. Allowing unauthorized access to Class Members' PII;

f. Failing to detect in a timely manner that Class Members' PII had been compromised; and

g. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

113. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' PII would result in injury to Class Members. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the investigation industry.

114. It was therefore foreseeable that the failure to adequately safeguard Class Members' PII would result in one or more types of injuries to Class Members.

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

116. Plaintiff 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) continue to provide adequate credit monitoring to all Class Members.

SECOND COUNT
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

117. Plaintiff repeats and re-alleges each and every allegation contained the Complaint as if fully set forth herein.

118. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as

Defendant's, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

119. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiff and Members of the Class due to the valuable nature of the PII at issue in this case—including Social Security numbers.

120. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

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

122. 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 its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and members of the Class.

123. As a direct and proximate result of Defendant's negligence per se, Plaintiff 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 PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (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 tax fraud and identity theft;

(vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remains 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 PII of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and members of the Class.

124. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and members of the Class have suffered and will suffer the continued risks of exposure of their PII, which remains 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 PII in its continued possession.

THIRD COUNT
Breach of Implied Contract
(On behalf of the Plaintiff and the Class)

125. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

126. Plaintiff and Class Members were required to provide their PII to Defendant as a condition of their employment with Defendant's partners.

127. Plaintiff and Class Members disclosed their PII in exchange for employment, along with Defendant's promise to protect their PII from unauthorized disclosure.

128. In its written privacy policies, Defendant Creative Services expressly promised Plaintiff and Class Members that it would only disclose PII under certain circumstances, none of which relate to the Data Breach.

129. Defendant further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PII would remain protected.

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

131. When Plaintiff and Class Members provided their PII to Defendant as a condition of employment, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

132. Defendant solicited, invited, and then required Class Members to provide their PII as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their PII to Defendant.

133. In entering into such implied contracts, Plaintiff 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.

134. Plaintiff and Class Members would not have entrusted their PII to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure. Plaintiff and Class Members would not have entrusted their PII 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.

135. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

136. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their PII.

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

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

139. Plaintiff 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 credit monitoring to all Class Members.

FOURTH COUNT
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

140. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth hereon.

141. Defendant benefited from receiving Plaintiff's and Class Members' PII by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

142. Defendant also understood and appreciated that Plaintiff's and Class Members' PII was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

143. Plaintiff and Class Members conferred a monetary benefit upon Defendant in the form of potential/actual employment, and in connection thereto, by providing their PII to Defendant with the understanding that Defendant would pay for the administrative costs of

reasonable data privacy and security practices and procedures. Specifically, they were required to provide Defendant with their PII. In exchange, Plaintiff and Class members should have received adequate protection and data security for such PII held by Defendant.

144. Defendant knew Plaintiff and Class members conferred a benefit which Defendant accepted. Defendant profited from their employment and used the PII of Plaintiff and Class Members for business purposes.

145. Defendant failed to provide reasonable security, safeguards, and protections to the PII of Plaintiff and Class Members.

146. Under the principles of equity and good conscience, Defendant should not be permitted to retain money belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures mandated by industry standards.

147. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiff and Class Members.

148. Defendant's enrichment at the expense of Plaintiff and Class Members is and was unjust.

149. As a result of Defendant's wrongful conduct, as alleged above, Plaintiff and the Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiff as Class Representative and his counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff 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 PII 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) Ordering Defendant to pay for not less than three years of credit monitoring services for Plaintiff and the Class;

f) For an award of actual damages, compensatory damages, in an amount to be determined, as allowable by law;

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

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

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

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

JURY TRIAL DEMANDED

Under the Massachusetts Rules of Civil Procedure 38, Plaintiff demands a trial by jury of any and all issues in this action so triable as of right.

Dated: March 3, 2022

Respectfully submitted,

/s/ Kurt J. Hagstrom, Esq.
Kurt J. Hagstrom, Esq.
BBO# 692154
Hagstrom Law Group
66 N. Second St.
New Bedford, MA 02740
Phone: (508) 612-4677
kurt@hagstromlawgroup.com

Terence R. Coates (*pro hac vice* forthcoming)
MARKOVITS, STOCK & DEMARCO, LLC
3825 Edwards Road, Suite 650
Cincinnati, OH 45209
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com

Joseph M. Lyon (*pro hac vice* forthcoming)
THE LYON FIRM
2754 Erie Avenue
Cincinnati, OH 45208
Phone: (513) 381-2333
Fax: (513) 721-1178
jlyon@thelyonfirm.com

Counsel for Plaintiff and the Putative Class