

#2

COMMONWEALTH OF MASSACHUSETTS

BRISTOL, ss.

SUPERIOR COURT DEPARTMENT

Santos Acosta, on behalf of himself and on  
behalf of all others similarly situated,

Plaintiff,

v.

Creative Services, Inc.,

Defendant.

Case No.: 2213CV00208C

BRISTOL, SS SUPERIOR COURT  
FILED

MAR 14 2022

MARC J. SANTOS, ESQ.  
CLERK/MAGISTRATE

**CLASS ACTION COMPLAINT**

Plaintiff Santos Acosta ("Plaintiff") brings this Class Action Complaint against Creative Services, Inc. ("Defendant" or "Creative Services"), in his individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

**INTRODUCTION**

1. Defendant is a company that conducts background checks for employment and licensing purposes. Creative Services obtains certain personally identifying information related to current and former employees, as well as employment candidates, of its customers in furtherance of the services it performs on behalf of its customers.

2. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard sensitive Personally Identifiable Information provided by its customers, including, without limitation, first and last names, dates of birth, Social Security numbers, and driver's license numbers ("PII").

3. On November 26, 2021, Defendant identified "potential unusual system activity" on its servers.<sup>1</sup> It later learned "that certain files may have been copied from Creative Service's

<sup>1</sup> <https://oag.ca.gov/system/files/Creative%20Services%2C%20Inc.%20-%20Sample%20Notice.pdf> (last visited Mar. 11, 2022).

systems on November 23, 2021 as part of a cyber-attack,” including the following sensitive data from Defendant’s customers’ employees and potential employees: “name and date of birth, Social Security number, and/or driver’s license number.” (the “Data Breach”).<sup>2</sup>

4. Defendant failed to use reasonable industry standard security measures, which would have prevented this type of attack from being successful. Defendant’s failure to use such measures is particularly egregious given the amount of highly sensitive PII that it maintains and the prevalence of data security incidents across the country.

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.

6. Hackers can access and then offer for sale this unencrypted, unredacted PII to criminals. The exposed PII of Plaintiff and Class Members can be sold on the dark web. Plaintiff and Class Members now face a present and continuing lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers.

7. Plaintiff bring this action on behalf of all persons whose PII was compromised as a result of Defendant’s failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of Defendant’s inadequate information security practices; and (iii) effectively secure its network containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant’s conduct amounts to negligence and violates federal and state statutes.

8. Plaintiff and Class Members have suffered injury as a result of Defendant’s conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; and (iv) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available

---

<sup>2</sup> *Id.*

for unauthorized third parties to access and abuse; and (b) may remain backed up 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.

9. The Federal Trade Commission ("FTC") recently stated that the types of PII that Creative Services collects and lost to criminals in this matter is "often used to commit identity theft and fraud":

For example, identity thieves use stolen names, addresses, and Social Security numbers to apply for credit cards in the victim's name. When the identity thief fails to pay credit card bills, the victim's credit suffers. Stolen personal information is also used to create phantom debt records used by debt collectors to harass consumers and demand payment for debts the consumers do not owe. Misappropriated bank account information can be used for unauthorized billing or fraudulent check scams. Identity thieves also use Social Security numbers and bank account information to intercept consumers' tax refunds fraudulently.<sup>3</sup>

10. Defendant disregarded the rights of Plaintiff and Class Members by recklessly or negligently failing to implement and maintain adequate and reasonable measures to ensure that the PII of Plaintiff and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data, even for internal use. As a result, the PII of Plaintiff and Class Members was compromised through disclosure to a known criminal organization. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

### **PARTIES**

#### ***Plaintiff Santos Acosta***

11. Plaintiff Santos Acosta is, and at all times relevant has been, a resident and citizen of Piermont, New York. Plaintiff received a "Notice of Data Incident" letter dated February 23, 2022, on or about that date.<sup>4</sup> The letter notified him that on November 26, 2021, Creative Services

---

<sup>3</sup> *Federal Trade Commission v. Immedia Solutions LLC et al.*, Case No. 2:22-cv-00073 (C.D. Cal. February 9, 2022).

<sup>4</sup> Exhibit A (Acosta Data Incident Notice).

determined that unauthorized persons “copied” from its systems files containing his PII, including his full name, date of birth, Social Security number, and/or driver’s license number.

12. The letter further advised that he should “remain vigilant against incidents of identity theft and fraud” by reviewing his account statements and monitoring credit reports “for suspicious activity.”

13. Upon information and belief, Defendant continues to maintain Plaintiff’s PII.

***Defendant Creative Services Inc.***

14. Defendant Creative Services, Inc., is a Massachusetts corporation that conducts commercial background screening with its principal place of business at 64 Pratt Street, Mansfield, Massachusetts 02048.

**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.

**FACTUAL ALLEGATIONS**

***Background***

18. Defendant is hired by companies across the nation (including New York) to conduct background screening procedures for licensing and employment purposes. It collects the PII of licensees and employees and potential employees from its commercial customers, including but not limited to individual’s full name, date of birth, Social Security number, and driver’s license number.

19. Plaintiff and Class Members, however, were not direct customers of Defendant.

20. Plaintiff and Class Members and/or Plaintiff's and Class Members' agents or employers relied on the sophistication of Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

21. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. In fact, Defendant was well aware of the dangers of a potential data breach: Only a few months earlier, Creative Services "became aware of unusual activity" in its systems and, on September 27, 2021, notified over one thousand individuals that their PII was "obtained by unauthorized person(s)."<sup>5</sup>

### ***The Data Breach***

22. On November 26, 2021, Defendant "became aware" of a second data breach in the same year: "[I]t was determined that certain files may have been copied from Creative Service's systems on November 23, 2021 as part of a cyber-attack."<sup>6</sup> According to Defendant, it then took steps to notify its customers and determine the contact information for impacted individuals, including Plaintiff and Class Members.<sup>7</sup> However, Defendant did not notify Plaintiff and the Class Members until over two months later, beginning in February 2022.<sup>8</sup>

23. Despite a protracted investigation into the Data Breach, assisted by the services of an unnamed cybersecurity firm, Defendant's only solutions to its inadequate safeguards are to provide notice to Plaintiff and the Class Members and to "work[] to enhance its technical security

---

<sup>5</sup> Data Breach Notice to the Maine Attorney General, archived at: [file:///T:/\\_MAB%20TEAM/\\_CASES/\\_DATA%20BREACH%20CASES/OC%20Creative%20Services/Creative%20Services%20Inc.%20-%20Notice%20of%20Data%20Event%20-%20ME.pdf](file:///T:/_MAB%20TEAM/_CASES/_DATA%20BREACH%20CASES/OC%20Creative%20Services/Creative%20Services%20Inc.%20-%20Notice%20of%20Data%20Event%20-%20ME.pdf) (last accessed Mar. 4, 2022).

<sup>6</sup> Exhibit B (Maine AG Notice).

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

tools.” This is not sufficient.

24. Defendant failed to use reasonable industry standard security measures, which would have prevented this type of attack. Defendant’s failure to use such measures is particularly egregious given the amount of highly sensitive PII that it maintains and the prevalence of data security incidents across the county.

25. In notice letters subsequently sent to victims of the Data Breach, Defendant acknowledged its duty to safeguard the PII in its possession, and the seriousness of the incident: “We take this incident and the security of personal information seriously.”<sup>9</sup>

26. The notice letters sent to victims of the Data Breach also acknowledged that its previous cybersecurity policies and procedures were lacking and need improvement: “[W]e are working to review our existing policies and procedures, including our information security plan, to evaluate additional measures and safeguards to protect against this type of incident in the future.”<sup>10</sup>

27. The notice letters to victims of the Data Breach did not provide the details of the Data Breach, the vulnerabilities exploited, or the remedial measures undertaken to ensure such a breach does not occur again.

28. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

29. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for many licensees, employees, and potential employees, such as encrypting the information or deleting it when it is no longer needed.<sup>11</sup>

---

<sup>9</sup> Ex. A.

<sup>10</sup> *Id.*

<sup>11</sup> It is clear that the information exposed in the Data Breach was unencrypted: California law requires companies to notify California residents “whose **unencrypted** personal information

30. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”<sup>12</sup>

31. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when

---

was, or is reasonably believed to have been, acquired by an unauthorized person” due to a “breach of the security of the system[.]” Cal. Civ. Code § 1798.82(a)(1) (emphasis added). Defendant notified the California Attorney General of the Data Breach on Feb. 23, 2022, evidencing that the exposed data was unencrypted.

<sup>12</sup> How to Protect Your Networks from RANSOMWARE, at 3, *available at*: <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Feb. 2, 2022).

necessary.

- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have written access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.<sup>13</sup>

32. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you

---

<sup>13</sup>

*Id.* at 3-4.



know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....

- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic....<sup>14</sup>

33. To prevent and detect cyber-attacks Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

**Thoroughly investigate and remediate alerts**

- Prioritize and treat commodity malware infections as potential full compromise;

---

<sup>14</sup> See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at*: <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Feb. 2, 2022).

### **Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

### **Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

### **Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

### **Harden infrastructure**

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].<sup>15</sup>

34. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of at least 164,673 individuals, including Plaintiff and Class Members. This does not include the number impacted by the data breach earlier in 2021.

### ***Defendant Acquires, Collects, and Stores the PII of Plaintiff and Class Members***

35. Defendant has historically acquired, collected, and stored the PII of Plaintiff and Class Members.

36. As part of receiving services from Defendant, Plaintiff's and Class Members' agents or employers, as customers of Defendant, are required to give their sensitive and confidential PII to Defendant. Defendant retains this information.

---

<sup>15</sup> See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at*: <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Feb. 2, 2022).

37. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

38. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and maintained securely, to use this information for business purposes only, and to make only authorized disclosures of this information.

39. Defendant could have prevented this Data Breach by properly and adequately securing and encrypting the files and file servers containing the PII of Plaintiff and Class Members.

40. Defendant's policies on its website include promises and legal obligations to maintain and protect PII, demonstrating an understanding of the importance of securing PII. For example:

- "CSI has established physical, electronic and procedural safeguards to protect personal information.";
- "CSI restricts access to personal information to those CSI employees who require access in order to perform their job responsibilities";
- "CSI conducts annual training regarding the lawful and intended purpose of processing sensitive information and the need to maintain the confidentiality of the sensitive information to which CSI employees have access"; and
- "Electronic personal information that is stored or transmitted is encrypted and layered for security by firewall and multi-tiered virus protection, as well as by network servers, network workstations and software applications that are password protected."

Although Defendant claims to encrypt "stored" information, considering the notice filed with the California Attorney General, that does not appear to be true for the 164,673 people impacted here.<sup>16</sup>

41. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is

---

<sup>16</sup> <https://www.creativeservices.com/about/resources/privacy-policy> (last visited Mar. 4, 2022).

exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data, and by Defendants very recent data breach earlier in 2021.

42. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

***Defendant Knew or Should Have Known of the Risk Because the Financial Industry is Particularly Susceptible to Cyber Attacks***

43. Defendant knew and understood unprotected or exposed PII in the custody of companies, such as Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that PII through unauthorized access.

44. Defendant had obligations created by contract, industry standards, common law, and representations made to Plaintiff and Class Members and/or to Plaintiff's and Class Members' agents or employers, and the general public, to keep their PII confidential and to protect it from unauthorized access and disclosure.

45. Plaintiff and Class Members and/or Plaintiff's and Class Members' agents or employers provided their PII to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with their obligations to keep such information confidential and secure from unauthorized access.

46. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches preceding the date of the breach.

47. Indeed, data breaches, such as the one experienced by Defendant, 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. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known and completely foreseeable to the public, including Defendant.

48. According to the FTC, identity theft wreaks havoc on consumers' finances, credit

history, and reputation and can take time, money, and patience to resolve.<sup>17</sup> Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.<sup>18</sup>

49. The PII of Plaintiff and Class Members was taken by hackers to engage in identity theft and/or to sell it to other criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years.

50. Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security systems were breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

51. Plaintiff and Class Members now currently face years of constant surveillance and monitoring of their financial and personal records and loss of rights. Plaintiff and Class Members are incurring, and will continue to incur, such damages in addition to any fraudulent use of their PII.

52. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members, such as encrypting the data so unauthorized third parties could not see the PII.

---

<sup>17</sup> See *Taking Charge. What to Do If Your Identity is Stolen*, FTC, 3 (Apr. 2013), <https://dss.mo.gov/cd/older-youth-program/files/taking-charge-what-to-do-if-identity-is-stolen.pdf> (last visited Feb. 2, 2022).

<sup>18</sup> *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. 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." *Id.*

### ***Defendant Failed to Comply with Industry Standards***

53. A number of industry and national best practices have been published and should have been used as a go-to resource and authoritative guide when developing Defendant's cybersecurity practices.

54. Best cybersecurity practices that are standard 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; and training staff regarding critical points.

55. Upon information and belief, Defendant failed to meet the minimum standards of the following cybersecurity frameworks: 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 established standards in reasonable cybersecurity readiness.

56. These foregoing frameworks are existing and applicable industry standards in Defendant's industry, and Defendant failed to comply with these accepted standards, thereby opening the door to a cyber-attack and causing the Data Breach.

### ***Value of Personally Identifiable Information***

57. The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."<sup>19</sup> 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

---

<sup>19</sup> 17 C.F.R. § 248.201 (2013).

number.”<sup>20</sup>

58. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. 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, and bank details have a price range of \$50 to \$200.<sup>21</sup> Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.<sup>22</sup> Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.<sup>23</sup>

59. Social Security numbers, for example, are among the worst kind of PII 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.<sup>24</sup>

60. It is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud

---

<sup>20</sup> *Id.*

<sup>21</sup> *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 visited Feb. 2, 2022).

<sup>22</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited Feb. 2, 2022).

<sup>23</sup> *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last visited Feb. 2, 2022).

<sup>24</sup> Social Security Administration, *Identity Theft and Your Social Security Number*, available at: <https://www.ssa.gov/pubs/EN-05-10064.pdf> (last visited Feb. 2, 2022).

activity to obtain a new number.

61. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, “[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.”<sup>25</sup>

62. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change—Social Security number, driver’s license number, name, and date of birth.

63. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”<sup>26</sup>

64. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

65. The fraudulent activity resulting from the Data Breach may not come to light for years.

66. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), 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

---

<sup>25</sup> Bryan Naylor, *Victims of Social Security Number Theft Find It’s Hard to Bounce Back*, NPR (Feb. 9, 2015), available at: <http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft> (last visited Feb. 2, 2022).

<sup>26</sup> Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last visited Feb. 2, 2022).



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.<sup>27</sup>

67. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

68. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

69. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's server(s), amounting to potentially thousands of individuals' detailed, PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

70. In the breach notification letter, Defendant made an offer of 12 months of credit monitoring and identity theft services. This is wholly inadequate to compensate Plaintiff and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, and medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiff's and Class Members' PII.

71. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

72. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class

---

<sup>27</sup> *Report to Congressional Requesters*. GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last visited Feb. 2, 2022).

Members are long lasting and severe. Once PII is stolen, particularly Social Security and driver's license numbers, fraudulent use of that information and damage to victims may continue for years.

***Plaintiff Santos Acosta Experience***

73. Plaintiff Acosta was required to provide and did provide his PII to Defendant as part of a background check for his employer from 2014 to 2016. The PII included his name, Social Security number, date of birth, and driver's license number.

74. To date, Defendant has done next to nothing to adequately protect Plaintiff Acosta and Class Members, or to compensate them for their injuries sustained in this Data Breach.

75. Defendant's data breach notice letter downplays the theft of Plaintiff's and Class Members' PII, when the facts demonstrate that the PII was targeted, accessed, and exfiltrated in a criminal cyberattack. The fraud and identity monitoring services offered by Defendant are only for one year, and it places the burden squarely on Plaintiff and Class Members by requiring them to expend time signing up for the service. Defendant also urges Plaintiff to spend more time reacting and remediating the impact of the breach caused by Defendant's inadequate safeguards when Defendant advised, in writing, that Plaintiff should "remain vigilant against incidents of identity theft and fraud" by reviewing his account statements and monitoring credit reports "for suspicious activity."

76. Plaintiff and Class Members have been further damaged by the compromise of their PII.

77. Plaintiff's PII was compromised in the Data Breach and was likely stolen and in the hands of cybercriminals who illegally accessed Defendant's network for the specific purpose of targeting the PII.

78. Plaintiff typically takes measures to protect his PII and is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or other unsecured source.

79. Plaintiff stores any documents containing his PII in a safe and secure location. And he diligently chooses unique usernames and passwords for his online accounts.

80. As a result of the Data Breach, Plaintiff has suffered a loss of time and has spent and continues to spend a considerable amount of time on issues related to this Data Breach. He monitors his accounts and credit scores, as he was directed to do by Defendant in the notice. This is time that was lost and unproductive and took away from other activities and work duties.

81. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that he and/or his agent or employer entrusted to Defendant for the purpose of obtaining services from Defendant, which was compromised in and as a result of the Data Breach.

82. Plaintiff 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.

83. Plaintiff has suffered continuing and certainly imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his Social Security Number, being placed in the hands of criminals.

84. Defendant obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Defendant required the PII from him and/or his agent or employer when they received services from Defendant. However, he would not have entrusted his PII to Defendant had he known that it would fail to maintain adequate data security. His PII was compromised and disclosed as a result of the Data Breach.

85. As a result of 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. As a result of the Data Breach, he is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come.

### **CLASS ALLEGATIONS**

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

87. 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").

88. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

89. Plaintiff reserves the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

90. Numerosity: The members of the Classes are so numerous that joinder of all members is impracticable, if not completely impossible. The Classes are apparently identifiable within Defendant's records.

91. Commonality: Common questions of law and fact exist as to all members of the Classes and predominate over any questions affecting solely individual members of the Classes. Among the questions of law and fact common to the Classes that predominate over questions which may affect individual Class Members, including the following:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;
- b. Whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendant had a duty not to use the PII of Plaintiff and Class Members for

non-business purposes;

- d. Whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. Whether and when Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
- h. 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;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual damages, statutory damages, and/or nominal damages as a result of Defendant's wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

92. Typicality: Plaintiff's claims are typical of those of the other members of the Classes because Plaintiff, like every other member, were exposed to virtually identical conduct and now suffers from the same violations of the law as other members of the Classes.

93. Adequacy: Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that he has no disabling conflicts of interest that would be antagonistic to those of the other Class Members. Plaintiff seek no relief that is antagonistic or adverse to the

Class Members and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff have retained counsel experienced in complex class action litigation, and Plaintiff intend to prosecute this action vigorously.

94. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Classes is impracticable. Individual damages for any individual Class Member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendant's misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

**FIRST COUNT**  
**NEGLIGENCE**

**(On Behalf of Plaintiff and the Class)**

95. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 94.

96. As a condition of receiving services from Defendant, Defendant's current and former customers were obligated to provide Defendant with Plaintiff's and Class Members' PII, including, but not limited to, first and last names, dates of birth, Social Security numbers, and driver's license numbers.

97. Plaintiffs and the Class entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

98. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

99. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party.

100. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiff and the Class in Defendant's possession was adequately secured and protected.

101. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former customers' PII that Defendant was no longer required to retain pursuant to regulations or legitimate business purposes.

102. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Class.

103. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant on the one hand and Plaintiff and the Class on the other. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential PII, a necessary part receiving services from Defendant.

104. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff or the Class.

105. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices, and Defendants prior data breach in 2021.

106. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that information, and the necessity for encrypting or redacting PII stored on Defendant's systems.

107. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included

its decisions to not comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendant.

108. Plaintiff and the Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

109. Defendant was in a position to protect against the harm suffered by Plaintiff and the Class as a result of the Data Breach.

110. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

111. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and the Class.

112. Defendant has admitted that the PII of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

113. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendant's possession or control.

114. Defendant improperly and inadequately safeguarded the PII of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

115. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Class in the face of increased risk of theft.

116. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former patients' PII.



117. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

118. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

119. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Class and the present harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PII of Plaintiff and the Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

120. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of 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 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 PII, 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 PII of Plaintiff and the Class; and (viii) 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 the Class.

121. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class 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.

122. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

123. Plaintiff and Class Members are therefore entitled to damages, including restitution and unjust enrichment, declaratory and injunctive relief, and attorneys' fees, costs, and expenses.

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

124. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 94.

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

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

127. In its written privacy policies, 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.

128. In its written privacy policies, Creative Services expressly promised Plaintiff and Class Members that it would encrypt PII under certain circumstances, but it did not.

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, and (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 or licensure, 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's 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, for example, (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.

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

140. Plaintiff re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 94.

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 payment for screening services, 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 payment for screening services 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, on himself and Class Members, requests judgment against Defendant and that the Court grant the following:

- A. For an order certifying the Class, as defined herein, and appointing Plaintiff and their Counsel to represent each such Class;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiff and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:
  - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
  - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

- iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;
- iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;
- v. prohibiting Defendant from maintaining the PII of Plaintiff and Class Members on a cloud-based database;
- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class

Members;

- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;
- xiii. requiring Defendant to implement a system of tests to assess its employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential PII to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment;

- D. For an award of damages, including actual, statutory, nominal, and consequential damages, as allowed by law in an amount to be determined;

- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and,
- G. Such other and further relief as this Court may deem just and proper.

**DEMAND FOR JURY TRIAL**

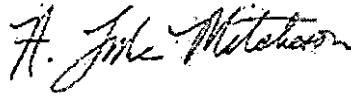
Plaintiff hereby demands that this matter be tried before a jury.

Respectfully Submitted,

The Plaintiff.

SANTOS ACOSTA, ON BEHALF OF HIMSELF AND ON  
BEHALF OF ALL OTHERS SIMILARY SITUATED,

By his attorneys,



H. Luke Mitcheson, BBO#: 676386  
**MORGAN & MORGAN**  
1601 Trapelo Road, Suite 174  
Waltham, MA 02451  
(857) 383-4905  
lmitcheson@forthepeople.com

Francesca Kester (*Pro hac vice forthcoming*)  
Jean S. Martin (*Pro hac vice forthcoming*)  
**MORGAN & MORGAN**  
**COMPLEX LITIGATION GROUP**  
210 N. Franklin St., Suite 700  
Tampa, FL 33602  
Telephone: (813) 559-4908  
Facsimile: (813) 222-4795  
jeanmartin@ForThePeople.com  
fkester@forthepeople.com

M. Anderson Berry (*Pro hac vice forthcoming*)  
Gregory Haroutunian (*Pro hac vice forthcoming*)  
**CLAYEO C. ARNOLD,**  
**A PROFESSIONAL LAW CORP.**  
865 Howe Avenue  
Sacramento, CA 95825  
Telephone: (916) 239-4778  
Facsimile: (916) 924-1829  
aberry@justice4you.com  
gharoutunian@justice4you.com