

1 Andrew G. Gunem (SBN: 354042)  
2 agunem@straussborrelli.com  
3 **STRAUSS BORRELLI PLLC**  
4 980 N. Michigan Avenue, Suite 1610  
Chicago, Illinois 60611  
Telephone: (872) 263-1100  
Facsimile: (872) 263-1109

5 *Attorney for Plaintiff and Proposed Class*

6  
7 **UNITED STATES DISTRICT COURT**  
8 **CENTRAL DISTRICT OF CALIFORNIA**  
**SOUTHERN DIVISION**

9 **JULIE SHIPP**, on behalf of herself and  
10 all others similarly situated,

11 Plaintiff,

12 v.

13 **CWS CAPITAL PARTNERS LLC,**  
14 **CWS APARTMENT HOMES LLC,**  
15 **and CWS CORPORATE HOUSING**  
**LLC,**

16 Defendants.

No. 8:24-cv-2552

**CLASS ACTION COMPLAINT**

1. NEGLIGENCE;
2. NEGLIGENCE *PER SE*;
3. BREACH OF IMPLIED CONTRACT;
4. BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING
5. UNJUST ENRICHMENT
6. CALIFORNIA’S UNFAIR COMPETITION LAW;
7. CALIFORNIA CONSUMER PRIVACY ACT;
8. CALIFORNIA CUSTOMER RECORDS ACT; AND
9. DECLARATORY JUDGMENT.

**DEMAND FOR JURY TRIAL**

1 Julie Shipp (“Plaintiff”), through her attorneys, individually and on behalf of  
2 all others similarly situated, brings this Class Action Complaint against Defendants  
3 CWS Capital Partners LLC, CWS Apartment Homes LLC, and CWS Corporate  
4 Housing LLC (“CWS” or “Defendants”), and their present, former, or future direct  
5 and indirect parent companies, subsidiaries, affiliates, agents, and/or other related  
6 entities. Plaintiff alleges the following on information and belief—except as to her  
7 own actions, counsel’s investigations, and facts of public record.

### 8 NATURE OF ACTION

9 1. This class action arises from Defendants’ failure to protect highly  
10 sensitive data.

11 2. Together, Defendants constitute a full-service real estate investment  
12 management business which owns and operates luxury apartments throughout the  
13 United States.<sup>1</sup> Defendants advertise “105 properties,” “29,000+ units,” and a  
14 portfolio value of “\$7+ billion.”<sup>2</sup>

15 3. As such, Defendants store a litany of highly sensitive personal  
16 identifiable information (“PII”) about their current and former tenants. But  
17 Defendants lost control over that data when cybercriminals infiltrated their  
18 insufficiently protected computer systems in a data breach (the “Data Breach”).

19 4. It is unknown for precisely how long the cybercriminals had access to  
20 Defendants’ network before the breach was discovered. In other words, Defendants  
21

---

22 <sup>1</sup> *Home Page*, CWS CAPITAL, <https://www.cwscapital.com/> (last visited Nov. 8,  
23 2024).

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

1 had no effective means to prevent, detect, stop, or mitigate breaches of their  
2 systems—thereby allowing cybercriminals unrestricted access to their current and  
3 former tenants’ PII.

4 5. On information and belief, cybercriminals were able to breach  
5 Defendants’ systems because Defendants failed to adequately train their employees  
6 on cybersecurity and failed to maintain reasonable security safeguards or protocols  
7 to protect the Class’s PII. In short, Defendants’ failures placed the Class’s PII in a  
8 vulnerable position—rendering them easy targets for cybercriminals.

9 6. Plaintiff is a Data Breach victim, having received a breach notice—  
10 attached as Exhibit A. She brings this class action on behalf of herself, and all others  
11 harmed by Defendants’ misconduct.

12 7. The exposure of one’s PII to cybercriminals is a bell that cannot be  
13 unrung. Before this data breach, their current and former tenants’ private  
14 information was exactly that—private. Not anymore. Now, their private  
15 information is forever exposed and unsecure.

16 **PARTIES**

17 8. Plaintiff, Julie Shipp, is a natural person and citizen of Texas where  
18 she intends to remain.

19 9. Defendant, CWS Capital Partners LLC, is a limited liability company  
20 formed under the laws of Delaware and with its principal place of business at 14  
21 Corporate Plaza Drive, Suite 210, Newport Beach, California 92660.

1 10. Defendant, CWS Apartment Homes LLC, is a limited liability  
2 company formed under the laws of Delaware and with its principal place of business  
3 at 14 Corporate Plaza Drive, Suite 210, Newport Beach, California 92660.

4 11. Defendant, CWS Corporate Housing LLC, is a limited liability  
5 company formed under the laws of Delaware and with its principal place of business  
6 at 106 E. Old Settlers Boulevard, Round Rock, Texas 78664.

7 **JURISDICTION AND VENUE**

8 12. This Court has subject matter jurisdiction over this action under the  
9 Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy  
10 exceeds \$5 million, exclusive of interest and costs. Plaintiff and Defendants are  
11 citizens of different states.<sup>3</sup> And there are over 100 putative Class Members.

12 13. This Court has personal jurisdiction over Defendants because CWS  
13 Capital Partners LLC and CWS Apartment Homes LLC have their principal place  
14 of business and/or corporate headquarters in California. Furthermore, all  
15

---

16 <sup>3</sup> Under the Class Action Fairness Act, “an unincorporated association shall be  
17 deemed to be a citizen of the State where it has its principal place of business and  
18 the State under whose laws it is organized.” 28 U.S.C. § 1332(d)(10); *see, e.g.,*  
19 *Calchi v. TopCo Assocs. LLC*, 676 F. Supp. 3d 604, 612 (N.D. Ill. 2023) (collecting  
20 cases) (“In a non-CAFA case, an LLC is a citizen where its members are citizens.  
21 But in a CAFA case, an LLC is a citizen of its state of organization and the state  
22 where it has its principal place of business.”); *Davis v. HSBC Bank Nevada NA*, 557  
23 F.3d 1026, 1032, & n.13 (9th Cir. 2009) (Kleinfeld, J., concurring) (discussing in  
24 dicta); *Abrego v. The Dow Chemical Co.*, 443 F.3d 676, 684 (9th Cir. 2006)  
(discussing in dicta). Thus, CWS Apartment Homes LLC and CWS Capital Partners  
LLC are citizens of Delaware (state of formation) and California (principal place of  
business). And CWS Corporate Housing LLC is a citizen of Delaware (state of  
formation) and Texas (principal place of business).

1 Defendants regularly conduct business in California and have sufficient minimum  
2 contacts in California.

3 14. Venue is proper in this Court because CWS Capital Partners LLC and  
4 CWS Apartment Homes LLC’s principal office is in this District, and because a  
5 substantial part of the events, acts, and omissions giving rise to Plaintiff’s claims  
6 occurred in this District.

7 **BACKGROUND**

8 ***Defendants Collected and Stored the PII of Plaintiff and the Class***

9 15. Together, Defendants constitute a full-service real estate investment  
10 management business which owns and operates luxury apartments throughout the  
11 United States.<sup>4</sup> Defendants advertise “105 properties,” “29,000+ units,” and a  
12 portfolio value of “\$7+ billion.”<sup>5</sup>

13 16. As part of their business, Defendants receive and maintain the PII of  
14 thousands of their current and former tenants.

15 17. In collecting and maintaining the PII, Defendants agreed they would  
16 safeguard the data in accordance with their internal policies, state law, and federal  
17 law. After all, Plaintiff and Class Members themselves took reasonable steps to  
18 secure their PII.

19 18. Under state and federal law, businesses like Defendants have duties to  
20 protect their current and former tenants’ PII and to notify them about breaches.

21  
22 <sup>4</sup> Home Page, CWS CAPITAL, <https://www.cwscapital.com/> (last visited Nov. 8,  
23 2024).

24 <sup>5</sup> *Id.*

1 19. Defendants recognize these duties, declaring in their “Privacy Notice  
2 and Policy” that:

3 a. “CWS Capital Partners (‘CWS’, ‘we’, and ‘us’) has created this  
4 Privacy Notice and Policy (‘Privacy Policy’) in order to  
5 demonstrate our commitment to protecting the personal  
6 information of (a) users of the CWS website (‘Site’) or the  
7 online services, systems or applications of CWS (collectively,  
8 ‘Services’); (b) our existing and prospective clients, and their  
9 personnel, users and representatives; and (c) any other  
10 individuals from whom we collect personal data during the  
11 course of our business activities.”<sup>6</sup>

12 b. “CWS will not share your personal information with third  
13 parties unless you have specifically requested that information  
14 be released to them or have otherwise consented to such  
15 sharing.”<sup>7</sup>

16 c. “CWS maintains appropriate physical, electronic and  
17 procedural safeguards and controls to help to protect against the  
18 loss, misuse, alteration and unauthorized disclosure of personal  
19 data in our possession or under our control. We periodically test  
20 the security protections of our information systems and monitor  
21

---

22 <sup>6</sup> *Privacy Notice and Policy*, CWS CAPITAL (Jan. 7, 2020)  
23 [https://www.cwscapital.com/static/media/documents/CWS\\_Privacy\\_Policy2.pdf](https://www.cwscapital.com/static/media/documents/CWS_Privacy_Policy2.pdf).

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

1 the effectiveness of our information security controls, systems  
2 and procedures.”<sup>8</sup>

3 20. In a separate “CWS Privacy Policy,” Defendant promise the following:

4 a. “This Privacy Policy details certain policies implemented  
5 throughout CWS governing CWS’ collection and use of  
6 personally identifiable information about users of the Site and  
7 our services.”<sup>9</sup>

8 b. “We may employ industry standard procedural and  
9 technological measures that are reasonably designed to help  
10 protect your personally identifiable information from loss,  
11 unauthorized access, disclosure, alteration or destruction.”<sup>10</sup>

12 c. “CWS may use, without limitation, firewalls, password  
13 protection, secure socket layer, and other security measures to  
14 help prevent unauthorized access to your personally identifiable  
15 information.”<sup>11</sup>

---

16  
17  
18  
19  
20 <sup>8</sup> *Id.*

21 <sup>9</sup> *CWS Privacy Policy*, CWS APARTMENTS (May 4, 2021) [https://g5-assets-cld-res.cloudinary.com/image/upload/v1620836651/g5/g5-c-5qfvlypqt-cws-apartment-homes/g5-cl-1lct5c19y-cws-apartment-homes-austin-tx/uploads/CWS\\_Privacy\\_Policy\\_ubn1mx.pdf](https://g5-assets-cld-res.cloudinary.com/image/upload/v1620836651/g5/g5-c-5qfvlypqt-cws-apartment-homes/g5-cl-1lct5c19y-cws-apartment-homes-austin-tx/uploads/CWS_Privacy_Policy_ubn1mx.pdf).

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

23 <sup>11</sup> *Id.*

1 ***Defendants’ Data Breach***

2 21. In or around July 27, 2022, Defendants were hacked in the Data  
3 Breach.<sup>12</sup>

4 22. Worryingly, Defendants already admitted that “unauthorized  
5 acquisition of your personal information could have occurred[.]”<sup>13</sup>

6 23. Because of Defendants’ Data Breach, at least the following types of  
7 PII were compromised:

- 8 a. names;
- 9 b. Social Security numbers;
- 10 c. account numbers; and
- 11 d. Driver’s license numbers.<sup>14</sup>

12 24. Additionally, in an official disclosure with the Massachusetts Office  
13 of Consumer Affairs and Business Regulation, Defendants responded “Yes” to the  
14 question “Mobile Device Lost Stolen” and indicated that the “Breach Type” was  
15 both “Paper” *and* “Electronic.”<sup>15</sup>

16 25. Currently, the precise number of persons injured is unclear. But upon  
17 information and belief, the size of the putative class can be ascertained from  
18 information in Defendants’ custody and control. And upon information and belief,

---

19  
20 <sup>12</sup> *Notice*, MASS.GOV, <https://www.mass.gov/doc/assigned-data-breach-number-28190-cws-apartment-homes-llc/download> (last visited Nov. 8, 2024).

21 <sup>13</sup> *Id.*

22 <sup>14</sup> *Data Breach Notification Report*, OFF. CONSUMER AFFAIRS & BUS. REG.,  
<https://www.mass.gov/doc/data-breach-report-2022/download> (last visited Nov. 8,  
23 2024).

24 <sup>15</sup> *Id.*

1 the putative class is over one hundred members—as it includes their current and  
2 former tenants.

3 26. In it unclear precisely when Defendants began issuing notice to Class  
4 Members. In their disclosures to the Massachusetts Office of Consumer Affairs and  
5 Business Regulation, Defendants:

- 6 a. reported a data breach under the name “CWS Apartment  
7 Homes, LLC” on September 2, 2022; and
- 8 b. reported a data breach under the name “CWS Corporate  
9 Housing LLC” on December 2, 2022.<sup>16</sup>

10 27. Thus, it appears that Defendants delayed notifying all Class Members  
11 by 128 days or more.<sup>17</sup> In doing so, Defendants kept the Class in the dark—thereby  
12 depriving the Class of the opportunity to try and mitigate their injuries in a timely  
13 manner.

14 28. And when Defendants did notify Plaintiff and the Class of the Data  
15 Breach, Defendants acknowledged that the Data Breach created a present,  
16 continuing, and significant risk of suffering identity theft, warning Plaintiff and the  
17 Class:

- 18 a. “You must place your request for a freeze with each of the three  
19 major consumer reporting agencies: Equifax

---

22 <sup>16</sup> *Id.*

23 <sup>17</sup> *Id.*

1 (www.equifax.com); Experian (www.experian.com); and  
2 TransUnion (www.transunion.com).”<sup>18</sup>

3 b. “[W]e encourage you to take advantage of the services being  
4 offered[.]”<sup>19</sup>

5 c. “We are providing you with steps we are taking in response to  
6 the incident and resources available to help you protect against  
7 the potential misuse of your information.”<sup>20</sup>

8 d. “You can further educate yourself regarding identity theft, fraud  
9 alerts, security freezes, and the steps you can take to protect  
10 yourself, by contacting the consumer reporting agencies, the  
11 Federal Trade Commission, or your state Attorney General. The  
12 Federal Trade Commission can be reached at: 600 Pennsylvania  
13 Avenue NW, Washington, DC 20580, www.identitytheft.gov,  
14 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261.”<sup>21</sup>

15 29. Defendants failed their duties when their inadequate security practices  
16 caused the Data Breach. In other words, Defendants’ negligence is evidenced by  
17 their failure to prevent the Data Breach and stop cybercriminals from accessing the  
18 PII. And thus, Defendants caused widespread injury and monetary damages.

19 \_\_\_\_\_  
20 <sup>18</sup> Notice, MASS.GOV, <https://www.mass.gov/doc/assigned-data-breach-number-28190-cws-apartment-homes-llc/download> (last visited Nov. 8, 2024).

21 <sup>19</sup> *Id.*

22 <sup>20</sup> Notice of Data Security Incident, MASS.GOV, <https://www.mass.gov/doc/assigned-data-breach-number-28664-cws-corporate-housing-llc/download> (last visited Nov. 8, 2024).

23 <sup>21</sup> *Id.*

1 30. Since the breach, Defendants have to have “moved quickly to  
2 investigate, respond, and confirm the security of our systems.”<sup>22</sup> But such simple  
3 declarations are insufficient to ensure that Plaintiff’s and Class Members’ PII will  
4 be protected from additional exposure in a subsequent data breach.

5 31. Further, the Notice of Data Breach shows that Defendants cannot—or  
6 will not—determine the full scope of the Data Breach, as Defendants have been  
7 unable to determine precisely what information was stolen and when.

8 32. Defendants have done little to remedy their Data Breach. True,  
9 Defendants have offered some victims credit monitoring and identity related  
10 services. But upon information and belief, such services are wholly insufficient to  
11 compensate Plaintiff and Class Members for the injuries that Defendants inflicted  
12 upon them.

13 33. Because of Defendants’ Data Breach, the sensitive PII of Plaintiff and  
14 Class Members was placed into the hands of cybercriminals—inflicting numerous  
15 injuries and significant damages upon Plaintiff and Class Members.

16 34. Upon information and belief, the cybercriminals in question are  
17 particularly sophisticated. After all, the cybercriminals: (1) defeated the relevant  
18 data security systems, (2) gained actual access to sensitive data, and (3) successfully  
19 accessed data.

20 35. And as the Harvard Business Review notes, such “[c]ybercriminals  
21 frequently use the Dark Web—a hub of criminal and illicit activity—to sell data  
22

---

23 <sup>22</sup> *Id.*

1 from companies that they have gained unauthorized access to through credential  
2 stuffing attacks, phishing attacks, [or] hacking.”<sup>23</sup>

3 36. Thus, on information and belief, Plaintiff’s and the Class’s stolen PII  
4 has already been published—or will be published imminently—by cybercriminals  
5 on the Dark Web.

6 ***Plaintiff’s Experiences and Injuries***

7 37. Plaintiff Julie Shipp is a former tenant of Defendants.

8 38. Thus, Defendants obtained and maintained Plaintiff’s PII.

9 39. As a result, Plaintiff was injured by Defendants’ Data Breach.

10 40. As a condition of her tenancy with Defendants, Plaintiff provided  
11 Defendants with her PII. Defendants used that PII to facilitate their provision of  
12 services and to obtain payment.

13 41. Plaintiff provided her PII to Defendants and trusted the company  
14 would use reasonable measures to protect it according to Defendants’ internal  
15 policies, as well as state and federal law. Defendants obtained and continue to  
16 maintain Plaintiff’s PII and have a continuing legal duty and obligation to protect  
17 that PII from unauthorized access and disclosure.

18 42. Plaintiff reasonably understood that a portion of the funds paid to  
19 Defendants would be used to pay for adequate cybersecurity and protection of PII.

---

21 <sup>23</sup> Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should*  
22 *You Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023)  
23 <https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back>.

1 43. Plaintiff received a Notice of Data Breach dated September 1, 2022.

2 The notice revealed the following.

3 a. “On July 27, 2022, an unknown individual burglarized certain  
4 employee offices at ‘The Nash.’”

5 b. “Among the items taken were two company laptop computers  
6 issued to leasing agent staff members.”

7 44. Through their Data Breach, Defendants compromised Plaintiff’s PII.

8 45. Thus, on information and belief, Plaintiff’s PII has already been  
9 published—or will be published imminently—by cybercriminals on the Dark Web.

10 46. In or around the timeframe of the Data Breach, Plaintiff resided in  
11 Defendants’ property. After the Data Breach, Defendants notified Plaintiff and  
12 Class Members that sensitive information was stolen in the Data Breach.

13 47. In the aftermath of the Data Breach, Plaintiff was evicted by  
14 Defendants—who claimed that Plaintiff had failed to pay rent. However, Plaintiff  
15 had paid her rent on time and in the correct amount.

16 48. Thus, on information and belief, Plaintiff’s eviction was the result of  
17 the Data Breach—and Defendants’ resulting inability to properly collect and/or  
18 process payments in the fallout of the Data Breach.

19 49. Defendants knew, or should have known, that Plaintiff had paid her  
20 rent on time and in the correct amount.

21 50. Plaintiff already suffered from fraud and identity theft.

22 a. On October 3, 2022, Plaintiff received a “Employment-Related  
23 Identity Theft Notice” letter from the IRS which warned her that

1 “[w]e believe another person may have used your Social  
2 Security number (SSN) to obtain employment.”

3 b. On August 21, 2024, Plaintiff was notified by the internet  
4 surveillance service “Experian IdentityWorks” that “[y]our  
5 Social Security number has been found on the dark web.”

6 c. On October 18, 2024, Plaintiff received an email notification  
7 from “NetCredit” which informed her that someone using her  
8 name had applied for a consumer credit loan from the creditor  
9 “Republic Bank & Trust Company.”

10 d. On November 12, 2024, Plaintiff was notified by the internet  
11 surveillance service “Experian IdentityWorks” that “your phone  
12 number has been found on the dark web” and that “identity  
13 thieves can gain access to your accounts by using your phone  
14 number[.]”

15 51. Plaintiff has spent—and will continue to spend—significant time and  
16 effort monitoring her accounts to protect herself from identity theft. After all,  
17 Defendants directed Plaintiff to take those steps in their breach notice.

18 52. And in the aftermath of the Data Breach, Plaintiff has suffered from a  
19 spike in spam and scam messages.

20 53. Plaintiff fears for her personal financial security and worries about  
21 what information was exposed in the Data Breach.

22 54. Because of Defendants’ Data Breach, Plaintiff has suffered—and will  
23 continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such

1 injuries go far beyond allegations of mere worry or inconvenience. Rather,  
2 Plaintiff's injuries are precisely the type of injuries that the law contemplates and  
3 addresses.

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

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

9 57. Plaintiff suffered imminent and impending injury arising from the  
10 substantially increased risk of fraud, misuse, and identity theft—all because  
11 Defendants' Data Breach placed Plaintiff's PII right in the hands of criminals.

12 58. Because of the Data Breach, Plaintiff anticipates spending  
13 considerable amounts of time and money to try and mitigate her injuries.

14 59. Today, Plaintiff has a continuing interest in ensuring that her PII—  
15 which, upon information and belief, remains backed up in Defendants'  
16 possession—is protected and safeguarded from additional breaches.

17 ***Plaintiff and the Proposed Class Face Significant Risk of Continued Identity***  
18 ***Theft***

19 60. Because of Defendants' failure to prevent the Data Breach, Plaintiff  
20 and Class Members suffered—and will continue to suffer—damages. These  
21 damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional  
22 distress. Also, they suffered or are at an increased risk of suffering:

- 23 a. loss of the opportunity to control how their PII is used;





1 68. Defendants’ failure to promptly and properly notify Plaintiff and Class  
2 Members of the Data Breach exacerbated Plaintiff and Class Members’ injury by  
3 depriving them of the earliest ability to take appropriate measures to protect their  
4 PII and take other necessary steps to mitigate the harm caused by the Data Breach.

5 ***Defendants Knew—Or Should Have Known—of the Risk of a Data Breach***

6 69. Defendants’ data security obligations were particularly important  
7 given the substantial increase in cyberattacks and/or data breaches in recent years.

8 70. In 2021, a record 1,862 data breaches occurred, exposing  
9 approximately 293,927,708 sensitive records—a 68% increase from 2020.<sup>24</sup>

10 71. Indeed, cyberattacks have become so notorious that the Federal Bureau  
11 of Investigation (“FBI”) and U.S. Secret Service issue warnings to potential targets,  
12 so they are aware of, and prepared for, a potential attack. As one report explained,  
13 “[e]ntities like smaller municipalities and hospitals are attractive to ransomware  
14 criminals . . . because they often have lesser IT defenses and a high incentive to  
15 regain access to their data quickly.”<sup>25</sup>

16 72. Therefore, the increase in such attacks, and attendant risk of future  
17 attacks, was widely known to the public and to anyone in Defendants’ industry,  
18 including Defendant.

19  
20  
21 <sup>24</sup> See *2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER  
(Jan. 2022) <https://notified.idtheftcenter.org/s/>.

22 <sup>25</sup> Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360  
23 (Nov. 18, 2019), <https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware>.

1 ***Defendants Failed to Follow FTC Guidelines***

2 73. According to the Federal Trade Commission (“FTC”), the need for  
3 data security should be factored into all business decision-making. Thus, the FTC  
4 issued numerous guidelines identifying best data security practices that  
5 businesses—like Defendant—should use to protect against unlawful data exposure.

6 74. In 2016, the FTC updated its publication, *Protecting Personal*  
7 *Information: A Guide for Business*. There, the FTC set guidelines for what data  
8 security principles and practices businesses must use.<sup>26</sup> The FTC declared that,  
9 *inter alia*, businesses must:

- 10 a. protect the personal customer information that they keep;
- 11 b. properly dispose of personal information that is no longer  
12 needed;
- 13 c. encrypt information stored on computer networks;
- 14 d. understand their network’s vulnerabilities; and
- 15 e. implement policies to correct security problems.

16 75. The guidelines also recommend that businesses watch for the  
17 transmission of large amounts of data out of the system—and then have a response  
18 plan ready for such a breach.

19 76. Furthermore, the FTC explains that companies must:

---

22 <sup>26</sup> *Protecting Personal Information: A Guide for Business*, FED TRADE  
23 COMMISSION (Oct. 2016) [https://www.ftc.gov/system/files/documents/plain-  
24 language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

- 1 a. not maintain information longer than is needed to authorize a
- 2 transaction;
- 3 b. limit access to sensitive data;
- 4 c. require complex passwords to be used on networks;
- 5 d. use industry-tested methods for security;
- 6 e. monitor for suspicious activity on the network; and
- 7 f. verify that third-party service providers use reasonable security
- 8 measures.

9 77. The FTC brings enforcement actions against businesses for failing to  
10 protect customer data adequately and reasonably. Thus, the FTC treats the failure—  
11 to use reasonable and appropriate measures to protect against unauthorized access  
12 to confidential consumer data—as an unfair act or practice prohibited by Section 5  
13 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting  
14 from these actions further clarify the measures businesses must take to meet their  
15 data security obligations.

16 78. In short, Defendants’ failure to use reasonable and appropriate  
17 measures to protect against unauthorized access to their current and former tenants’  
18 data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15  
19 U.S.C. § 45.

20 ***Defendants Failed to Follow Industry Standards***

21 79. Several best practices have been identified that—at a *minimum*—  
22 should be implemented by businesses like Defendant. These industry standards  
23 include: educating all employees; strong passwords; multi-layer security, including

1 firewalls, anti-virus, and anti- malware software; encryption (making data  
2 unreadable without a key); multi-factor authentication; backup data; and limiting  
3 which employees can access sensitive data.

4 80. Other industry standard best practices include: installing appropriate  
5 malware detection software; monitoring and limiting the network ports; protecting  
6 web browsers and email management systems; setting up network systems such as  
7 firewalls, switches, and routers; monitoring and protection of physical security  
8 systems; protection against any possible communication system; and training staff  
9 regarding critical points.

10 81. Upon information and belief, Defendants failed to implement industry-  
11 standard cybersecurity measures, including failing to meet the minimum standards  
12 of both the NIST Cybersecurity Framework Version 2.0 (including without  
13 limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01,  
14 PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01,  
15 DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04) and the Center for  
16 Internet Security’s Critical Security Controls (CIS CSC), which are all established  
17 standards in reasonable cybersecurity readiness.

18 82. These frameworks are applicable and accepted industry standards. And  
19 by failing to comply with these accepted standards, Defendants opened the door to  
20 the criminals—thereby causing the Data Breach.

21 **CLASS ACTION ALLEGATIONS**

22 83. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2),  
23 and 23(b)(3), individually and on behalf of all members of the following class:

1  
2 All individuals residing in the United States whose PII  
3 was compromised in the Data Breach discovered by CWS  
4 in July 2022.

5  
6 84. Excluded from the Class are Defendant, their agents, affiliates, parents,  
7 subsidiaries, any entity in which Defendants have a controlling interest, any  
8 Defendants officer or director, any successor or assign, and any Judge who  
9 adjudicates this case, including their staff and immediate family.

10 85. Plaintiff reserves the right to amend the class definition.

11 86. Certification of Plaintiff's claims for class-wide treatment is  
12 appropriate because Plaintiff can prove the elements of her claims on class-wide  
13 bases using the same evidence as would be used to prove those elements in  
14 individual actions asserting the same claims.

15 87. Ascertainability. All members of the proposed Class are readily  
16 ascertainable from information in Defendants' custody and control. After all,  
17 Defendants already identified some individuals and sent them data breach notices.

18 88. Numerosity. The Class Members are so numerous that joinder of all  
19 Class Members is impracticable. Upon information and belief, the proposed Class  
20 includes at least 100 members.

21 89. Typicality. Plaintiff's claims are typical of Class Members' claims as  
22 each arises from the same Data Breach, the same alleged violations by Defendant,  
23 and the same unreasonable manner of notifying individuals about the Data Breach.



- 1 h. what the proper damages measure is; and
- 2 i. if Plaintiff and the Class are entitled to damages, treble damages,
- 3 and or injunctive relief.

4 92. Superiority. A class action will provide substantial benefits and is  
5 superior to all other available means for the fair and efficient adjudication of this  
6 controversy. The damages or other financial detriment suffered by individual Class  
7 Members are relatively small compared to the burden and expense that individual  
8 litigation against Defendants would require. Thus, it would be practically  
9 impossible for Class Members, on an individual basis, to obtain effective redress  
10 for their injuries. Not only would individualized litigation increase the delay and  
11 expense to all parties and the courts, but individualized litigation would also create  
12 the danger of inconsistent or contradictory judgments arising from the same set of  
13 facts. By contrast, the class action device provides the benefits of adjudication of  
14 these issues in a single proceeding, ensures economies of scale, provides  
15 comprehensive supervision by a single court, and presents no unusual management  
16 difficulties.

17 **FIRST CAUSE OF ACTION**  
18 **Negligence**  
19 **(On Behalf of Plaintiff and the Class)**

20 93. Plaintiff incorporates by reference all other paragraphs as if fully set  
21 forth herein.

22 94. Plaintiff and the Class entrusted their PII to Defendants on the premise  
23 and with the understanding that Defendants would safeguard their PII, use their PII

1 for business purposes only, and/or not disclose their PII to unauthorized third  
2 parties.

3 95. Defendants owed a duty of care to Plaintiff and Class Members  
4 because it was foreseeable that Defendants' failure—to use adequate data security  
5 in accordance with industry standards for data security—would compromise their  
6 PII in a data breach. And here, that foreseeable danger came to pass.

7 96. Defendants have full knowledge of the sensitivity of the PII and the  
8 types of harm that Plaintiff and the Class could and would suffer if their PII was  
9 wrongfully disclosed.

10 97. Defendants owed these duties to Plaintiff and Class Members because  
11 they are members of a well-defined, foreseeable, and probable class of individuals  
12 whom Defendants knew or should have known would suffer injury-in-fact from  
13 Defendants' inadequate security practices. After all, Defendants actively sought and  
14 obtained Plaintiff and Class Members' PII.

15 98. Defendants owed—to Plaintiff and Class Members—at least the  
16 following duties to:

- 17 a. exercise reasonable care in handling and using the PII in their  
18 care and custody;
- 19 b. implement industry-standard security procedures sufficient to  
20 reasonably protect the information from a data breach, theft, and  
21 unauthorized;
- 22 c. promptly detect attempts at unauthorized access;
- 23

1 d. notify Plaintiff and Class Members within a reasonable  
2 timeframe of any breach to the security of their PII.

3 99. Thus, Defendants owed a duty to timely and accurately disclose to  
4 Plaintiff and Class Members the scope, nature, and occurrence of the Data Breach.  
5 After all, this duty is required and necessary for Plaintiff and Class Members to take  
6 appropriate measures to protect their PII, to be vigilant in the face of an increased  
7 risk of harm, and to take other necessary steps to mitigate the harm caused by the  
8 Data Breach.

9 100. Defendants also had a duty to exercise appropriate clearinghouse  
10 practices to remove PII it was no longer required to retain under applicable  
11 regulations.

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

16 102. Defendants' duty to use reasonable security measures arose because of  
17 the special relationship that existed between Defendants and Plaintiff and the Class.  
18 That special relationship arose because Plaintiff and the Class entrusted Defendants  
19 with their confidential PII, a necessary part of obtaining services from Defendant.

20 103. The risk that unauthorized persons would attempt to gain access to the  
21 PII and misuse it was foreseeable. Given that Defendants hold vast amounts of PII,  
22 it was inevitable that unauthorized individuals would attempt to access Defendants'  
23 databases containing the PII—whether by malware or otherwise.

1 104. PII is highly valuable, and Defendants knew, or should have known,  
2 the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and  
3 Class Members' and the importance of exercising reasonable care in handling it.

4 105. Defendants improperly and inadequately safeguarded the PII of  
5 Plaintiff and the Class in deviation of standard industry rules, regulations, and  
6 practices at the time of the Data Breach.

7 106. Defendants breached these duties as evidenced by the Data Breach.

8 107. Defendants acted with wanton and reckless disregard for the security  
9 and confidentiality of Plaintiff's and Class Members' PII by:

10 a. disclosing and providing access to this information to third  
11 parties and

12 b. failing to properly supervise both the way the PII was stored,  
13 used, and exchanged, and those in their employ who were  
14 responsible for making that happen.

15 108. Defendants breached their duties by failing to exercise reasonable care  
16 in supervising their agents, contractors, vendors, and suppliers, and in handling and  
17 securing the personal information and PII of Plaintiff and Class Members which  
18 actually and proximately caused the Data Breach and Plaintiff and Class Members'  
19 injury.

20 109. Defendants further breached their duties by failing to provide  
21 reasonably timely notice of the Data Breach to Plaintiff and Class Members, which  
22 actually and proximately caused and exacerbated the harm from the Data Breach  
23 and Plaintiff and Class Members' injuries-in-fact.

1 110. Defendants have admitted that the PII of Plaintiff and the Class was  
2 wrongfully lost and disclosed to unauthorized third persons because of the Data  
3 Breach.

4 111. As a direct and traceable result of Defendants' negligence and/or  
5 negligent supervision, Plaintiff and Class Members have suffered or will suffer  
6 damages, including monetary damages, increased risk of future harm,  
7 embarrassment, humiliation, frustration, and emotional distress.

8 112. And, on information and belief, Plaintiff's PII has already been  
9 published—or will be published imminently—by cybercriminals on the Dark  
10 Web.

11 113. Defendants' breach of their common-law duties to exercise reasonable  
12 care and their failures and negligence actually and proximately caused Plaintiff and  
13 Class Members actual, tangible, injury-in-fact and damages, including, without  
14 limitation, the theft of their PII by criminals, improper disclosure of their PII, lost  
15 benefit of their bargain, lost value of their PII, and lost time and money incurred to  
16 mitigate and remediate the effects of the Data Breach that resulted from and were  
17 caused by Defendants' negligence, which injury-in-fact and damages are ongoing,  
18 imminent, immediate, and which they continue to face.

19 **SECOND CAUSE OF ACTION**  
20 ***Negligence per se***  
21 **(On Behalf of Plaintiff and the Class)**

22 114. Plaintiff incorporates by reference all other paragraphs as if fully set  
23 forth herein.

1 115. Under the FTC Act, 15 U.S.C. § 45, Defendants had a duty to use fair  
2 and adequate computer systems and data security practices to safeguard Plaintiff’s  
3 and Class Members’ PII.

4 116. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting  
5 commerce,” including, as interpreted and enforced by the FTC, the unfair act or  
6 practice by businesses, such as Defendant, of failing to use reasonable measures to  
7 protect the PII entrusted to it. The FTC publications and orders promulgated  
8 pursuant to the FTC Act also form part of the basis of Defendants’ duty to protect  
9 Plaintiff and the Class Members’ sensitive PII.

10 117. Defendants breached their respective duties to Plaintiff and Class  
11 Members under the FTC Act by failing to provide fair, reasonable, or adequate  
12 computer systems and data security practices to safeguard PII.

13 118. Defendants violated their duty under Section 5 of the FTC Act by  
14 failing to use reasonable measures to protect PII and not complying with applicable  
15 industry standards as described in detail herein. Defendants’ conduct was  
16 particularly unreasonable given the nature and amount of PII Defendants had  
17 collected and stored and the foreseeable consequences of a data breach, including,  
18 specifically, the immense damages that would result to individuals in the event of a  
19 breach, which ultimately came to pass.

20 119. The harm that has occurred is the type of harm the FTC Act is intended  
21 to guard against. Indeed, the FTC has pursued numerous enforcement actions  
22 against businesses that, because of their failure to employ reasonable data security  
23

1 measures and avoid unfair and deceptive practices, caused the same harm as that  
2 suffered by Plaintiff and members of the Class.

3 120. But for Defendants' wrongful and negligent breach of their duties  
4 owed, Plaintiff and Class Members would not have been injured.

5 121. The injury and harm suffered by Plaintiff and Class Members was the  
6 reasonably foreseeable result of Defendants' breach of their duties. Defendants  
7 knew or should have known that Defendants were failing to meet their duties and  
8 that their breach would cause Plaintiff and members of the Class to suffer the  
9 foreseeable harms associated with the exposure of their PII.

10 122. Defendants' various violations and their failure to comply with  
11 applicable laws and regulations constitutes negligence *per se*.

12 123. As a direct and proximate result of Defendants' negligence *per se*,  
13 Plaintiff and Class Members have suffered and will continue to suffer numerous  
14 injuries (as detailed *supra*).

15 **THIRD CAUSE OF ACTION**  
16 **Breach of Implied Contract**  
**(On Behalf of Plaintiff and the Class)**

17 124. Plaintiff incorporates by reference all other paragraphs as if fully set  
18 forth herein.

19 125. Plaintiff and Class Members were required to provide their PII to  
20 Defendants as a condition of receiving services provided by Defendant. Plaintiff  
21 and Class Members provided their PII to Defendants or their third-party agents in  
22 exchange for Defendants' services.  
23

1 126. Plaintiff and Class Members reasonably understood that a portion of  
2 the funds they paid would be used to pay for adequate cybersecurity measures.

3 127. Plaintiff and Class Members reasonably understood that Defendants  
4 would use adequate cybersecurity measures to protect the PII that they were  
5 required to provide based on Defendants' duties under state and federal law and  
6 their internal policies.

7 128. Plaintiff and the Class Members accepted Defendants' offers by  
8 disclosing their PII to Defendants or their third-party agents in exchange for  
9 services.

10 129. In turn, and through internal policies, Defendants agreed to protect and  
11 not disclose the PII to unauthorized persons.

12 130. In their Privacy Policies, Defendants represented that they had a legal  
13 duty to protect Plaintiff's and Class Member's PII.

14 131. Implicit in the parties' agreement was that Defendants would provide  
15 Plaintiff and Class Members with prompt and adequate notice of all unauthorized  
16 access and/or theft of their PII.

17 132. After all, Plaintiff and Class Members would not have entrusted their  
18 PII to Defendants in the absence of such an agreement with Defendant.

19 133. Plaintiff and the Class fully performed their obligations under the  
20 implied contracts with Defendant.

21 134. The covenant of good faith and fair dealing is an element of every  
22 contract. Thus, parties must act with honesty in fact in the conduct or transactions  
23 concerned. Good faith and fair dealing, in connection with executing contracts and

1 discharging performance and other duties according to their terms, means  
2 preserving the spirit—and not merely the letter—of the bargain. In short, the parties  
3 to a contract are mutually obligated to comply with the substance of their contract  
4 in addition to its form.

5 135. Subterfuge and evasion violate the duty of good faith in performance  
6 even when an actor believes their conduct to be justified. Bad faith may be overt or  
7 consist of inaction. And fair dealing may require more than honesty.

8 136. Defendants materially breached the contracts it entered with Plaintiff  
9 and Class Members by:

- 10 a. failing to safeguard their information;
- 11 b. failing to notify them promptly of the intrusion into their  
12 computer systems that compromised such information.
- 13 c. failing to comply with industry standards;
- 14 d. failing to comply with the legal obligations necessarily  
15 incorporated into the agreements; and
- 16 e. failing to ensure the confidentiality and integrity of the  
17 electronic PII that Defendants created, received, maintained,  
18 and transmitted.

19 137. In these and other ways, Defendants violated their duty of good faith  
20 and fair dealing.

21 138. Defendants' material breaches were the direct and proximate cause of  
22 Plaintiff's and Class Members' injuries (as detailed *supra*).  
23

1 139. And, on information and belief, Plaintiff's PII has already been  
2 published—or will be published imminently—by cybercriminals on the Dark Web.

3 140. Plaintiff and Class Members performed as required under the relevant  
4 agreements, or such performance was waived by Defendants' conduct.

5 **FOURTH CAUSE OF ACTION**  
6 **Breach of the Implied Covenant of Good Faith and Fair Dealing**  
7 **(On Behalf of Plaintiff and the Class)**

8 141. Plaintiff incorporates by reference all other paragraphs as if fully set  
9 forth herein.

10 142. Under California law, every contract imposes on each party a duty of  
11 good faith and fair dealing in each performance and their enforcement. Thus, parties  
12 must act with honesty in fact in the conduct or transactions concerned. Good faith  
13 and fair dealing, in connection with executing contracts and discharging  
14 performance and other duties according to their terms, means preserving the spirit—  
15 and not merely the letter—of the bargain. In short, the parties to a contract are  
16 mutually obligated to comply with the substance of their contract in addition to their  
17 form.

18 143. Subterfuge and evasion violate the duty of good faith in performance  
19 even when an actor believes their conduct to be justified. Bad faith may be overt or  
20 consist of inaction. And fair dealing may require more than honesty.

21 144. Here, Plaintiff and Defendant entered into a contract (implied in law,  
22 fact, or otherwise) whereby Defendant agreed to:

- 23 a. use a portion of the funds paid by Plaintiff and Class Members  
24 would be used to pay for adequate cybersecurity measures;





1 Members, on the other hand, suffered as a direct and proximate result of  
2 Defendants' failure to provide the requisite security.

3 156. Under principles of equity and good conscience, Defendants should  
4 not be permitted to retain the full value of Plaintiff's and Class Members' (1) PII  
5 and (2) payment because Defendants failed to adequately protect their PII.

6 157. Plaintiff and Class Members have no adequate remedy at law.

7 158. Defendants should be compelled to disgorge into a common fund—for  
8 the benefit of Plaintiff and Class Members—all unlawful or inequitable proceeds  
9 that they received because of their misconduct.

10  
11 **SIXTH CAUSE OF ACTION**  
12 **Violation of California's Unfair Competition Law (UCL)**  
13 **Cal. Bus. & Prof. Code § 17200, *et seq.***  
14 **(On Behalf of Plaintiff and the Class)**

15 159. Plaintiff incorporates by reference all other paragraphs as if fully set  
16 forth herein.

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

20 161. Defendants' conduct is unlawful because it violates the California  
21 Consumer Privacy Act of 2018, Civ. Code § 1798.100, *et seq.* (the "CCPA") and  
22 the California Customer Records Act, Cal. Civ. Code § 1798.80, *et seq.* (the  
23 "CRA"), and other state data security laws.

24 162. Defendants stored the PII of Plaintiff and the Class in their computer  
systems and knew or should have known that they did not employ reasonable,

1 industry standard, and appropriate security measures that complied with applicable  
2 regulations and that would have kept Plaintiff's and the Class's PII secure to prevent  
3 the loss or misuse of that PII.

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

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

13 165. Had Defendants complied with these requirements, Plaintiff and the  
14 Class would not have suffered the damages related to the data breach.

15 166. Defendants' conduct was unlawful, in that they violated the CCPA.

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

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

21 169. Defendants' conduct is an unfair business practice under the UCL  
22 because it was immoral, unethical, oppressive, and unscrupulous and caused  
23

1 substantial harm. This conduct includes employing unreasonable and inadequate  
2 data security despite their business model of actively collecting PII.

3 170. Defendants also engaged in unfair business practices under the  
4 “tethering test.” Its actions and omissions, as described above, violated fundamental  
5 public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code §  
6 1798.1 (“The Legislature declares that . . . all individuals have a right of privacy in  
7 information pertaining to them . . . The increasing use of computers . . . has greatly  
8 magnified the potential risk to individual privacy that can occur from the  
9 maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the  
10 intent of the Legislature to ensure that personal information about California  
11 residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the intent of the  
12 Legislature that this chapter [including the Online Privacy Protection Act] is a  
13 matter of statewide concern.”). Defendants’ acts and omissions thus amount to a  
14 violation of the law.

15 171. Instead, Defendants made the PII of Plaintiff and the Class accessible  
16 to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and  
17 the Class to an impending risk of identity theft. Additionally, Defendants’ conduct  
18 was unfair under the UCL because it violated the policies underlying the laws set  
19 out in the prior paragraph.

20 172. As a result of those unlawful and unfair business practices, Plaintiff  
21 and the Class suffered an injury-in-fact and have lost money or property.  
22  
23

1 173. For one, on information and belief, Plaintiff’s and the Class’s stolen  
2 PII has already been published—or will be published imminently—by  
3 cybercriminals on the dark web.

4 174. The injuries to Plaintiff and the Class greatly outweigh any alleged  
5 countervailing benefit to consumers or competition under all of the circumstances.

6 175. There were reasonably available alternatives to further Defendants’  
7 legitimate business interests, other than the misconduct alleged in this complaint.

8 176. Therefore, Plaintiff and the Class are entitled to equitable relief,  
9 including restitution of all monies paid to or received by Defendants; disgorgement  
10 of all profits accruing to Defendants because of their unfair and improper business  
11 practices; a permanent injunction enjoining Defendants’ unlawful and unfair  
12 business activities; and any other equitable relief the Court deems proper.

13 **SEVENTH CAUSE OF ACTION**  
14 **Violations of the California Consumer Privacy Act (“CCPA”)**  
15 **Cal. Civ. Code § 1798.150**  
**(On Behalf of Plaintiff and the Class)**

16 177. Plaintiff incorporates by reference all other paragraphs as if fully set  
17 forth herein.

18 178. Defendants violated California Civil Code § 1798.150 of the CCPA by  
19 failing to implement and maintain reasonable security procedures and practices  
20 appropriate to the nature of the information to protect the nonencrypted PII of  
21 Plaintiff and the Class. As a direct and proximate result, Plaintiff’s and the Class’s  
22 nonencrypted and nonredacted PII was subject to unauthorized access and  
23 exfiltration, theft, or disclosure.

1 179. Defendants are each a “business” under the meaning of Civil Code §  
2 1798.140 because Defendants are each a “corporation, association, or other legal  
3 entity that is organized or operated for the profit or financial benefit of their  
4 shareholders or other owners” that “collects consumers’ personal information” and  
5 is active “in the State of California” and “had annual gross revenues in excess of  
6 twenty-five million dollars (\$25,000,000) in the preceding calendar year.” Civil  
7 Code § 1798.140(d).

8 180. Plaintiff and Class Members seek injunctive or other equitable relief  
9 to ensure Defendants hereinafter adequately safeguards PII by implementing  
10 reasonable security procedures and practices. Such relief is particularly important  
11 because Defendants continue to hold PII, including Plaintiff’s and Class Members’  
12 PII. Plaintiff and Class Members have an interest in ensuring that their PII is  
13 reasonably protected, and Defendants have demonstrated a pattern of failing to  
14 adequately safeguard this information.

15 181. Pursuant to California Civil Code § 1798.150(b), Plaintiff mailed a  
16 CCPA notice letter to Defendants’ registered service agents, detailing the specific  
17 provisions of the CCPA that Defendants have violated and continues to violate. If  
18 Defendants cannot cure within 30 days—and Plaintiff believes such cure is not  
19 possible under these facts and circumstances—then Plaintiff intends to promptly  
20 amend this Complaint to seek statutory damages as permitted by the CCPA.

21 182. As described herein, an actual controversy has arisen and now exists  
22 as to whether Defendants implemented and maintained reasonable security  
23

1 procedures and practices appropriate to the nature of the information so as to protect  
2 the personal information under the CCPA.

3 183. A judicial determination of this issue is necessary and appropriate at  
4 this time under the circumstances to prevent further data breaches by Defendants.

5 **EIGHTH CAUSE OF ACTION**  
6 **Violation of the California Customer Records Act**  
7 **Cal. Civ. Code § 1798.80, *et seq.***  
8 **(On Behalf of Plaintiff and the Class)**

9 184. Plaintiff incorporates by reference all other paragraphs as if fully set  
10 forth herein.

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

21 186. The Data Breach constitutes a “breach of the security system” of  
22 Defendants.

23 187. An unauthorized person acquired the personal, unencrypted  
24 information of Plaintiff and the Class.

1 188. Defendants knew that an unauthorized person had acquired the  
2 personal, unencrypted information of Plaintiff and the Class but waited  
3 approximately 128 days or more to notify them. Given the severity of the Data  
4 Breach, this was an unreasonable delay.

5 189. Defendants' unreasonable delay prevented Plaintiff and the Class from  
6 taking appropriate measures from protecting themselves against harm.

7 190. Because Plaintiff and the Class were unable to protect themselves, they  
8 suffered incrementally increased damages that they would not have suffered with  
9 timelier notice.

10 191. Plaintiff and the Class are entitled to equitable relief and damages in  
11 an amount to be determined at trial.

12 **NINTH CAUSE OF ACTION**  
13 **Declaratory Judgment**  
**(On Behalf of Plaintiff and the Class)**

14 192. Plaintiff incorporates by reference all other paragraphs as if fully set  
15 forth herein.

16 193. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this  
17 Court is authorized to enter a judgment declaring the rights and legal relations of  
18 the parties and to grant further necessary relief. The Court has broad authority to  
19 restrain acts, such as those alleged herein, which are tortious and unlawful.

20 194. In the fallout of the Data Breach, an actual controversy has arisen about  
21 Defendants' various duties to use reasonable data security. On information and  
22 belief, Plaintiff alleges that Defendants' actions were—and *still* are—inadequate  
23

1 and unreasonable. And Plaintiff and Class Members continue to suffer injury from  
2 the ongoing threat of fraud and identity theft.

3 195. Given its authority under the Declaratory Judgment Act, this Court  
4 should enter a judgment declaring, among other things, the following:

- 5 a. Defendants owed—and continue to owe—a legal duty to use  
6 reasonable data security to secure the data entrusted to it;
- 7 b. Defendants have a duty to notify impacted individuals of the  
8 Data Breach under the common law and Section 5 of the FTC  
9 Act;
- 10 c. Defendants breached, and continue to breach, their duties by  
11 failing to use reasonable measures to the data entrusted to it; and
- 12 d. Defendants breach of their duties caused—and continue to  
13 cause—injuries to Plaintiff and Class Members.

14 196. The Court should also issue corresponding injunctive relief requiring  
15 Defendants to use adequate security consistent with industry standards to protect  
16 the data entrusted to it.

17 197. If an injunction is not issued, Plaintiff and the Class will suffer  
18 irreparable injury and lack an adequate legal remedy if Defendants experience a  
19 second data breach.

20 198. And if a second breach occurs, Plaintiff and the Class will lack an  
21 adequate remedy at law because many of the resulting injuries are not readily  
22 quantified in full and they will be forced to bring multiple lawsuits to rectify the  
23 same conduct. Simply put, monetary damages—while warranted for out-of-pocket

1 damages and other legally quantifiable and provable damages—cannot cover the  
2 full extent of Plaintiff and Class Members’ injuries.

3 199. If an injunction is not issued, the resulting hardship to Plaintiff and  
4 Class Members far exceeds the minimal hardship that Defendants could experience  
5 if an injunction is issued.

6 200. An injunction would benefit the public by preventing another data  
7 breach—thus preventing further injuries to Plaintiff, Class Members, and the public  
8 at large.

9 **PRAYER FOR RELIEF**

10 Plaintiff and Class Members respectfully request judgment against  
11 Defendants and that the Court enter an order:

- 12 A. Certifying this case as a class action on behalf of Plaintiff and the  
13 proposed Class, appointing Plaintiff as class representative, and  
14 appointing her counsel to represent the Class;
- 15 B. Awarding declaratory and other equitable relief as necessary to protect  
16 the interests of Plaintiff and the Class;
- 17 C. Awarding injunctive relief as necessary to protect the interests of  
18 Plaintiff and the Class;
- 19 D. Enjoining Defendants from further unfair and/or deceptive practices;
- 20 E. Awarding Plaintiff and the Class damages including applicable  
21 compensatory, exemplary, punitive damages, and statutory damages,  
22 as allowed by law;
- 23

- 1 F. Awarding restitution and damages to Plaintiff and the Class in an  
2 amount to be determined at trial;
- 3 G. Awarding attorneys' fees and costs, as allowed by law;
- 4 H. Awarding prejudgment and post-judgment interest, as provided by  
5 law;
- 6 I. Granting Plaintiff and the Class leave to amend this complaint to  
7 conform to the evidence produced at trial; and
- 8 J. Granting other relief that this Court finds appropriate.

9 **DEMAND FOR JURY TRIAL**

10 Plaintiff demands a jury trial for all claims so triable.

11  
12 Dated: November 21, 2024

Respectfully submitted,

13  
14 By: /s/ Andrew G. Gunem

Andrew G. Gunem (SBN: 354042)

**STRAUSS BORRELLI PLLC**

980 N. Michigan Avenue, Suite 1610

Chicago, Illinois 60611

Telephone: (872) 263-1100

Facsimile: (872) 263-1109

15  
16  
17  
18 agunem@straussborrelli.com

19 *Attorney for Plaintiff and Proposed Class*