

UNITED STATES DISTRICT COURT  
DISTRICT OF ARIZONA

Alexxi Guyette, on behalf of herself and all  
others similarly situated,

Plaintiff,

v.

Enroll Confidently, Inc.,

Defendant.

No.

**CLASS ACTION COMPLAINT**

**FOR DAMAGES, INJUNCTIVE  
RELIEF, AND EQUITABLE  
RELIEF FOR:**

- 1. NEGLIGENCE;**
- 2. BREACH OF IMPLIED  
CONTRACT;**
- 3. INVASION OF PRIVACY;**
- 4. UNJUST ENRICHMENT;**
- 5. BREACH OF FIDUCIARY  
DUTY;**
- 6. VIOLATION OF THE  
ARIZONA CONSUMER  
FRAUD ACT; AND**
- 7. DECLARATORY  
JUDGMENT.**

**DEMAND FOR JURY TRIAL**

Alexxi Guyette (“Plaintiff”), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Enroll Confidently, Inc. (“Enroll” or “Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities. Plaintiff alleges the following on information and belief—except as to her own actions, counsel’s investigations, and facts of public record.

**NATURE OF ACTION**

1  
2 1. This class action arises from Defendant’s failure to protect highly sensitive  
3 data.

4 2. Defendant is an Arizona-based corporation that “provides a benefits  
5 enrollment platform to support employers and benefits providers throughout the employee  
6 enrollment process.”<sup>1</sup> As such, consumers “who seek to obtain an employer-sponsored  
7 product enroll in the benefit offering via [defendant’s] Platform.”<sup>2</sup>

8 3. As such, Defendant stores a litany of highly sensitive personal identifiable  
9 information (“PII”) and protected health information (“PHI”)—together “PII/PHI”—  
10 about its current and former consumers. But Defendant lost control over that data when  
11 cybercriminals infiltrated its insufficiently protected computer systems in a data breach  
12 (the “Data Breach”).

13 4. It is unknown for precisely how long the cybercriminals had access to  
14 Defendant’s network before the breach was discovered. In other words, Defendant had no  
15 effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby  
16 allowing cybercriminals unrestricted access to its current and former consumers’ PII/PHI.

17 5. On information and belief, cybercriminals were able to breach Defendant’s  
18 systems because Defendant failed to adequately train its employees on cybersecurity and  
19 failed to maintain reasonable security safeguards or protocols to protect the Class’s

20  
21 <sup>1</sup> *Notice of Data Event*, ENROLL CONFIDENTLY,  
<https://www.enrollconfidently.com/Content/NoticeOfBreach.pdf> (last visited August 27,  
2024).

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

1 PII/PHI. In short, Defendant’s failures placed the Class’s PII/PHI in a vulnerable  
2 position—rendering them easy targets for cybercriminals.

3 6. Plaintiff is a Data Breach victim, having received a breach notice—attached  
4 as Exhibit A. She brings this class action on behalf of herself, and all others harmed by  
5 Defendant’s misconduct.

6 7. The exposure of one’s PII/PHI to cybercriminals is a bell that cannot be  
7 unrung. Before this data breach, its current and former consumers’ private information  
8 was exactly that—private. Not anymore. Now, their private information is forever exposed  
9 and unsecure.

10 **PARTIES**

11 8. Plaintiff, Alexxi Guyette, is a natural person and citizen of Vermont where  
12 she intends to remain.

13 9. Defendant, Enroll Confidently, Inc., is a for-profit corporation incorporated  
14 in Delaware with its principal place of business at 13924 E Dyer Lane, Unit 4020,  
15 Scottsdale, Arizona 85262.

16 **JURISDICTION AND VENUE**

17 10. This Court has subject matter jurisdiction over this action under the Class  
18 Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds \$5  
19 million, exclusive of interest and costs. Plaintiff and Defendant are citizens of different  
20 states. And there are over 100 putative Class members.

1 11. This Court has personal jurisdiction over Defendant because it is  
2 headquartered in Arizona, regularly conducts business in Arizona, and has sufficient  
3 minimum contacts in Arizona.

4 12. Venue is proper in this Court because Defendant’s principal office is in this  
5 District, and because a substantial part of the events, acts, and omissions giving rise to  
6 Plaintiff’s claims occurred in this District.

7 **BACKGROUND**

8 *Defendant Collected and Stored the PII/PHI of Plaintiff and the Class*

9 13. Defendant is an Arizona-based corporation that “provides a benefits  
10 enrollment platform to support employers and benefits providers throughout the employee  
11 enrollment process.”<sup>3</sup> As such, consumers “who seek to obtain an employer-sponsored  
12 product enroll in the benefit offering via [defendant’s] Platform.”<sup>4</sup>

13 14. As part of its business, Defendant receives and maintains the PII/PHI of  
14 thousands of its current and former consumers.

15 15. In collecting and maintaining the PII/PHI, Defendant agreed it would  
16 safeguard the data in accordance with its internal policies, state law, and federal law. After  
17 all, Plaintiff and Class members themselves took reasonable steps to secure their PII/PHI.

18 16. Under state and federal law, businesses like Defendant have duties to protect  
19 its current and former consumers’ PII/PHI and to notify them about breaches.

20 \_\_\_\_\_  
21 <sup>3</sup> *Notice of Data Event*, ENROLL CONFIDENTLY,  
<https://www.enrollconfidently.com/Content/NoticeOfBreach.pdf> (last visited August 27,  
2024).

22 <sup>4</sup> *Id.*

1           17. Throughout its website, Defendant often references a “Privacy Policy.”<sup>5</sup>  
2 However, a Privacy Policy cannot be found on Defendant’s website. Upon information  
3 and belief, Defendant’s Privacy Policy was active at all relevant times and evinced  
4 Defendant’s duty to use reasonable data security practices and to follow applicable privacy  
5 laws.

6           18. Furthermore, Defendant’s CEO—Thomas McKiernan—is also the CEO of  
7 “Ep6ix” which is a “end-to-end benefits communication, education, and enrollment  
8 partner.”<sup>6</sup> Notably, Ep6ix has a “partnership[.]” with Defendant and advertises that  
9 Defendant’s “Platform Features” include the “[t]ransmission of files to carrier and broker  
10 through *secure FTP* [file transfer protocol.]”<sup>7</sup> Thus, upon information and belief,  
11 Defendant similarly advertises that it provides reasonable data security.

### 12 ***Defendant’s Data Breach***

13           19. On February 13, 2024, Defendant was hacked in the Data Breach.<sup>8</sup>  
14  
15  
16

---

17 <sup>5</sup> See e.g., *About*, ENROLL CONFIDENTLY, <https://www.enrollconfidently.com/About> (last  
18 visited August 27, 2024); *Terms of Use*, ENROLL CONFIDENTLY,  
<https://www.enrollconfidently.com/TermsOfUse> (last visited August 27, 2024).

19 <sup>6</sup> Thomas McKiernan, LINKEDIN, <https://www.linkedin.com/in/mckiernanthomas> (last  
20 visited August 27, 2024); *About Us*, EP6IX, <https://ep6ix.com/about-us/> (last visited  
21 August 27, 2024).

22 <sup>7</sup> *About Us*, EP6IX, <https://ep6ix.com/enrollment-technology-solutions/> (last visited  
23 August 27, 2024).

<sup>8</sup> *Notice of Data Event*, ENROLL CONFIDENTLY,  
<https://www.enrollconfidently.com/Content/NoticeOfBreach.pdf> (last visited August 27,  
2024).

1           20.   Worryingly, Defendant already admitted that “an unauthorized actor gained  
2 access to the network on February 13, 2024 and, during that time, *copied certain files*  
3 from the system.”<sup>9</sup>

4           21.   Because of Defendant’s Data Breach, at least the following types of PII/PHI  
5 were compromised:

- 6           a.   names;
- 7           b.   dates of birth;
- 8           c.   Social Security numbers;
- 9           d.   driver’s license numbers;
- 10          e.   state identification numbers;
- 11          f.   financial account information;
- 12          g.   health insurance information; and
- 13          h.   medical information.<sup>10</sup>

14          22.   Currently, the precise number of persons injured is unclear. But upon  
15 information and belief, the size of the putative class can be ascertained from information  
16 in Defendant’s custody and control. And upon information and belief, the putative class  
17 is over one hundred members—as it includes its current and former consumers.

---

18  
19  
20  
21  
22       <sup>9</sup> *Id.*

23       <sup>10</sup> *Id.*

1 23. Indeed, in Texas alone, the Data Breach exposed the PII/PHI of 2,590  
2 people.<sup>11</sup>

3 24. And yet, Defendant waited over until August 16, 2024, before it began  
4 notifying the class—over six months after the Data Breach was discovered.<sup>12</sup>

5 25. Thus, Defendant kept the Class in the dark—thereby depriving the Class of  
6 the opportunity to try and mitigate their injuries in a timely manner.

7 26. And when Defendant did notify Plaintiff and the Class of the Data Breach,  
8 Defendant acknowledged that the Data Breach created a present, continuing, and  
9 significant risk of suffering identity theft, warning Plaintiff and the Class:

10 a. “Enroll Confidently encourages individuals who may be affected to  
11 remain vigilant against incidents of identity theft and fraud by  
12 reviewing account statements and monitoring free credit reports for  
13 suspicious activity and to detect errors.”

14 b. “Individuals are also encouraged to review the Steps Individuals Can  
15 Take To Protect Personal Information section below.”

16 c. “[To] educate themselves regarding identity theft, fraud alerts, credit  
17 freezes, and the steps they can take to protect your personal  
18  
19  
20

---

21 <sup>11</sup> *Data Security Breach Reports*, ATTY GEN TEXAS,  
<https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage> (last  
22 visited August 27, 2024).

<sup>12</sup> *Id.*; see also Ex. A.

1 information by contacting the consumer reporting bureaus, the  
2 Federal Trade Commission, or their state Attorney General.”<sup>13</sup>

3 27. Defendant failed its duties when its inadequate security practices caused the  
4 Data Breach. In other words, Defendant’s negligence is evidenced by its failure to prevent  
5 the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Defendant  
6 caused widespread injury and monetary damages.

7 28. Since the breach, Defendant has declared that it is “working to enhance its  
8 existing security measures to further protect its systems moving forward.”<sup>14</sup>

9 29. However, mere claims of “working to enhance” data security does not  
10 establish that Defendant *actually enhanced* its data security to a sufficient level. Thus,  
11 injunctive relief is necessary to ensure that Defendant institutes adequate data security to  
12 protect the PII/PHI that it still retains.

13 30. Defendant has done little to remedy its Data Breach. True, Defendant has  
14 offered some victims credit monitoring and identity related services. But upon information  
15 and belief, such services are wholly insufficient to compensate Plaintiff and Class  
16 members for the injuries that Defendant inflicted upon them.

17 31. Because of Defendant’s Data Breach, the sensitive PII/PHI of Plaintiff and  
18 Class members was placed into the hands of cybercriminals—inflicting numerous injuries  
19 and significant damages upon Plaintiff and Class members.

20  
21 \_\_\_\_\_  
<sup>13</sup> *Id.*

22 <sup>14</sup> *Id.*



1           32. Upon information and belief, the cybercriminals in question are particularly  
2 sophisticated. After all, the cybercriminals: (1) defeated the relevant data security systems,  
3 (2) gained actual access to sensitive data, and (3) successfully *copied* data.

4           33. And as the Harvard Business Review notes, such “[c]ybercriminals  
5 frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from  
6 companies that they have gained unauthorized access to through credential stuffing  
7 attacks, phishing attacks, [or] hacking.”<sup>15</sup>

8           34. Thus, on information and belief, Plaintiff’s and the Class’s stolen PII/PHI  
9 has already been published—or will be published imminently—by cybercriminals on the  
10 Dark Web.

11 ***Plaintiff’s Experiences and Injuries***

12           35. Plaintiff Alexxi Guyette provided his PII/PHI to Defendant to obtain  
13 employee-related benefits pursuant to her employment with Cafua Management Company  
14 LLC. As a result, Plaintiff was injured by Defendant’s Data Breach when her PII/PHI was  
15 compromised.

16           36. Defendant used Plaintiff’s PII/PHI to facilitate its provision of products and  
17 services.

18           37. Plaintiff provided her PII/PHI to Defendant and trusted the company would  
19 use reasonable measures to protect it according to Defendant’s internal policies, as well  
20

---

21 <sup>15</sup> Brenda R. Sharton, *Your Company’s Data Is for Sale on the Dark Web. Should You*  
22 *Buy It Back?*, HARVARD BUS. REV. (Jan. 4, 2023) [https://hbr.org/2023/01/your-](https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back)  
23 [companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back](https://hbr.org/2023/01/your-companys-data-is-for-sale-on-the-dark-web-should-you-buy-it-back).

1 as state and federal law. Defendant obtained and continues to maintain Plaintiff's PII/PHI  
2 and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized  
3 access and disclosure.

4 38. Plaintiff reasonably understood that a portion of the funds paid to Defendant  
5 would be used to pay for adequate cybersecurity and protection of PII/PHI.

6 39. Plaintiff does not recall ever learning that her information was compromised  
7 in a data breach incident—other than the breach at issue here.

8 40. Plaintiff received a Notice of Data Breach on August 26, 2024.

9 41. Thus, on information and belief, Plaintiff's PII/PHI has already been  
10 published—or will be published imminently—by cybercriminals on the Dark Web.

11 42. Plaintiff has spent—and will continue to spend—significant time and effort  
12 monitoring her accounts to protect herself from identity theft. After all, Defendant directed  
13 Plaintiff to take those steps in its breach notice.

14 43. Specifically, Plaintiff spent approximately two (2) hours—which otherwise  
15 would have been dedicated to employment and/or leisure—calling the various credit  
16 bureaus to institute fraud alerts.

17 44. And in the aftermath of the Data Breach, Plaintiff has suffered from a spike  
18 in scam emails and text messages which appear to be targeted phishing attempts (e.g.,  
19 messages purportedly about lost packages).

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

1 46. Because of Defendant’s Data Breach, Plaintiff has suffered—and will  
2 continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such  
3 injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff’s  
4 injuries are precisely the type of injuries that the law contemplates and addresses.

5 47. Plaintiff suffered actual injury from the exposure and theft of her PII/PHI—  
6 which violates her rights to privacy.

7 48. Plaintiff suffered actual injury in the form of damages to and diminution in  
8 the value of her PII/PHI. After all, PII/PHI is a form of intangible property—property that  
9 Defendant was required to adequately protect.

10 49. Plaintiff suffered imminent and impending injury arising from the  
11 substantially increased risk of fraud, misuse, and identity theft—all because Defendant’s  
12 Data Breach placed Plaintiff’s PII/PHI right in the hands of criminals.

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

15 51. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—  
16 which, upon information and belief, remains backed up in Defendant’s possession—is  
17 protected and safeguarded from additional breaches.

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

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

- 1 a. loss of the opportunity to control how their PII/PHI is used;
- 2 b. diminution in value of their PII/PHI;
- 3 c. compromise and continuing publication of their PII/PHI;
- 4 d. out-of-pocket costs from trying to prevent, detect, and recovery from
- 5 identity theft and fraud;
- 6 e. lost opportunity costs and wages from spending time trying to
- 7 mitigate the fallout of the Data Breach by, *inter alia*, preventing,
- 8 detecting, contesting, and recovering from identify theft and fraud;
- 9 f. delay in receipt of tax refund monies;
- 10 g. unauthorized use of their stolen PII/PHI; and
- 11 h. continued risk to their PII/PHI—which remains in Defendant’s
- 12 possession—and is thus as risk for futures breaches so long as
- 13 Defendant fails to take appropriate measures to protect the PII/PHI.

14 53. Stolen PII/PHI is one of the most valuable commodities on the criminal  
15 information black market. According to Experian, a credit-monitoring service, stolen  
16 PII/PHI can be worth up to \$1,000.00 depending on the type of information obtained.

17 54. The value of Plaintiff and Class’s PII/PHI on the black market is  
18 considerable. Stolen PII/PHI trades on the black market for years. And criminals  
19 frequently post and sell stolen information openly and directly on the “Dark Web”—  
20 further exposing the information.

21 55. It can take victims years to discover such identity theft and fraud. This gives  
22 criminals plenty of time to sell the PII/PHI far and wide.

1           56. One way that criminals profit from stolen PII/PHI is by creating  
2 comprehensive dossiers on individuals called “Fullz” packages. These dossiers are both  
3 shockingly accurate and comprehensive. Criminals create them by cross-referencing and  
4 combining two sources of data—first the stolen PII/PHI, and second, unregulated data  
5 found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

6           57. The development of “Fullz” packages means that the PII/PHI exposed in the  
7 Data Breach can easily be linked to data of Plaintiff and the Class that is available on the  
8 internet.

9           58. In other words, even if certain information such as emails, phone numbers,  
10 or credit card numbers may not be included in the PII/PHI stolen by the cyber-criminals  
11 in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price  
12 to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and  
13 over. That is exactly what is happening to Plaintiff and Class members, and it is reasonable  
14 for any trier of fact, including this Court or a jury, to find that Plaintiff and other Class  
15 members’ stolen PII/PHI is being misused, and that such misuse is fairly traceable to the  
16 Data Breach.

17           59. Defendant disclosed the PII/PHI of Plaintiff and Class members for  
18 criminals to use in the conduct of criminal activity. Specifically, Defendant opened up,  
19 disclosed, and exposed the PII/PHI of Plaintiff and Class members to people engaged in  
20 disruptive and unlawful business practices and tactics, including online account hacking,  
21 unauthorized use of financial accounts, and fraudulent attempts to open unauthorized  
22 financial accounts (i.e., identity fraud), all using the stolen PII/PHI.

1           60. Defendant's failure to promptly and properly notify Plaintiff and Class  
2 members of the Data Breach exacerbated Plaintiff and Class members' injury by depriving  
3 them of the earliest ability to take appropriate measures to protect their PII/PHI and take  
4 other necessary steps to mitigate the harm caused by the Data Breach.

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

6           61. Defendant's data security obligations were particularly important given the  
7 substantial increase in cyberattacks and/or data breaches in recent years.

8           62. In 2021, a record 1,862 data breaches occurred, exposing approximately  
9 293,927,708 sensitive records—a 68% increase from 2020.<sup>16</sup>

10           63. Indeed, cyberattacks have become so notorious that the Federal Bureau of  
11 Investigation (“FBI”) and U.S. Secret Service issue warnings to potential targets, so they  
12 are aware of, and prepared for, a potential attack. As one report explained, “[e]ntities like  
13 smaller municipalities and hospitals are attractive to ransomware criminals . . . because  
14 they often have lesser IT defenses and a high incentive to regain access to their data  
15 quickly.”<sup>17</sup>

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

---

19  
20 <sup>16</sup> See *2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) <https://notified.idtheftcenter.org/s/>.

21 <sup>17</sup> Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18,  
22 2019), [https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-](https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware)  
23 [targeted-ransomware](https://www.law360.com/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware).

1 ***Defendant Failed to Follow FTC Guidelines***

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

6 66. In 2016, the FTC updated its publication, *Protecting Personal Information:  
7 A Guide for Business*. There, the FTC set guidelines for what data security principles and  
8 practices businesses must use.<sup>18</sup> The FTC declared that, *inter alia*, businesses must:

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

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

17 68. Furthermore, the FTC explains that companies must:

- 18 a. not maintain information longer than is needed to authorize a  
19 transaction;

---

21 <sup>18</sup> *Protecting Personal Information: A Guide for Business*, FED TRADE COMMISSION  
22 (Oct. 2016) [https://www.ftc.gov/system/files/documents/plain-language/pdf-  
0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).

- 1 b. limit access to sensitive data;
- 2 c. require complex passwords to be used on networks;
- 3 d. use industry-tested methods for security;
- 4 e. monitor for suspicious activity on the network; and
- 5 f. verify that third-party service providers use reasonable security
- 6 measures.

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

13 70. In short, Defendant’s failure to use reasonable and appropriate measures to  
14 protect against unauthorized access to its current and former consumers’ data constitutes  
15 an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

16 ***Defendant Failed to Follow Industry Standards***

17 71. Several best practices have been identified that—at a *minimum*—should be  
18 implemented by businesses like Defendant. These industry standards include: educating  
19 all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and  
20 anti- malware software; encryption (making data unreadable without a key); multi-factor  
21 authentication; backup data; and limiting which employees can access sensitive data.



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

6           73. Defendant failed to meet the minimum standards of any of the following  
7 frameworks: the NIST Cybersecurity Framework Version 1.1 (including without  
8 limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1,  
9 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  
10 RS.CO-2), and the Center for Internet Security’s Critical Security Controls (CIS CSC),  
11 which are all established standards in reasonable cybersecurity readiness.

12           74. These frameworks are applicable and accepted industry standards. And by  
13 failing to comply with these accepted standards, Defendant opened the door to the  
14 criminals—thereby causing the Data Breach.

15 ***Defendant Violated HIPAA***

16           75. HIPAA circumscribes security provisions and data privacy responsibilities  
17 designed to keep patients’ medical information safe. HIPAA compliance provisions,  
18 commonly known as the Administrative Simplification Rules, establish national standards  
19  
20  
21  
22  
23

1 for electronic transactions and code sets to maintain the privacy and security of protected  
2 health information.<sup>19</sup>

3 76. HIPAA provides specific privacy rules that require comprehensive  
4 administrative, physical, and technical safeguards to ensure the confidentiality, integrity,  
5 and security of PII/PHI and PHI is properly maintained.<sup>20</sup>

6 77. The Data Breach itself resulted from a combination of inadequacies showing  
7 Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security  
8 failures include, but are not limited to:

- 9 a. failing to ensure the confidentiality and integrity of electronic PHI  
10 that it creates, receives, maintains and transmits in violation of 45  
11 C.F.R. § 164.306(a)(1);
- 12 b. failing to protect against any reasonably-anticipated threats or  
13 hazards to the security or integrity of electronic PHI in violation of  
14 45 C.F.R. § 164.306(a)(2);
- 15 c. failing to protect against any reasonably anticipated uses or  
16 disclosures of electronic PHI that are not permitted under the privacy  
17 rules regarding individually identifiable health information in  
18 violation of 45 C.F.R. § 164.306(a)(3);

---

19  
20 <sup>19</sup> HIPAA lists 18 types of information that qualify as PHI according to guidance from the  
21 Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*:  
22 names, addresses, any dates including dates of birth, Social Security numbers, and medical  
23 record numbers.

<sup>20</sup> See 45 C.F.R. § 164.306 (security standards and general rules); 45 C.F.R. § 164.308  
(administrative safeguards); 45 C.F.R. § 164.310 (physical safeguards); 45 C.F.R. §  
164.312 (technical safeguards).

- 1 d. failing to ensure compliance with HIPAA security standards by  
2 Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- 3 e. failing to implement technical policies and procedures for electronic  
4 information systems that maintain electronic PHI to allow access  
5 only to those persons or software programs that have been granted  
6 access rights in violation of 45 C.F.R. § 164.312(a)(1);
- 7 f. failing to implement policies and procedures to prevent, detect,  
8 contain and correct security violations in violation of 45 C.F.R. §  
9 164.308(a)(1);
- 10 g. failing to identify and respond to suspected or known security  
11 incidents and failing to mitigate, to the extent practicable, harmful  
12 effects of security incidents that are known to the covered entity in  
13 violation of 45 C.F.R. § 164.308(a)(6)(ii);
- 14 h. failing to effectively train all staff members on the policies and  
15 procedures with respect to PHI as necessary and appropriate for staff  
16 members to carry out their functions and to maintain security of PHI  
17 in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5);  
18 and
- 19 i. failing to design, implement, and enforce policies and procedures  
20 establishing physical and administrative safeguards to reasonably  
21 safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).
- 22
- 23

1 78. Simply put, the Data Breach resulted from a combination of insufficiencies  
2 that demonstrate Defendant failed to comply with safeguards mandated by HIPAA  
3 regulations.

4 **CLASS ACTION ALLEGATIONS**

5 79. Plaintiff brings this class action under Fed. R. Civ. P. 23(a), 23(b)(2), and  
6 23(b)(3), individually and on behalf of all members of the following class:

7 All individuals residing in the United States whose PII/PHI  
8 was compromised in the Data Breach discovered by Enroll  
9 Confidently, Inc. in February 2024, including all those  
10 individuals who received notice of the breach.

11 80. Excluded from the Class are Defendant, its agents, affiliates, parents,  
12 subsidiaries, any entity in which Defendant has a controlling interest, any Defendant  
13 officer or director, any successor or assign, and any Judge who adjudicates this case,  
14 including their staff and immediate family.

15 81. Plaintiff reserves the right to amend the class definition.

16 82. Certification of Plaintiff's claims for class-wide treatment is appropriate  
17 because Plaintiff can prove the elements of her claims on class-wide bases using the same  
18 evidence as would be used to prove those elements in individual actions asserting the same  
19 claims.

20 83. Ascertainability. All members of the proposed Class are readily  
21 ascertainable from information in Defendant's custody and control. After all, Defendant  
22 already identified some individuals and sent them data breach notices.  
23



- 1 d. if Defendant breached contract promises to safeguard Plaintiff and
- 2 the Class's PII/PHI;
- 3 e. if Defendant took reasonable measures to determine the extent of the
- 4 Data Breach after discovering it;
- 5 f. if Defendant's Breach Notice was reasonable;
- 6 g. if the Data Breach caused Plaintiff and the Class injuries;
- 7 h. what the proper damages measure is; and
- 8 i. if Plaintiff and the Class are entitled to damages, treble damages, and
- 9 or injunctive relief.

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

22 **FIRST CAUSE OF ACTION**

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

1  
2           89. Plaintiff incorporates by reference all other paragraphs as if fully set forth  
3 herein.

4           90. Plaintiff and the Class (or their third-party agents) entrusted their PII/PHI to  
5 Defendant on the premise and with the understanding that Defendant would safeguard  
6 their PII/PHI, use their PII/PHI for business purposes only, and/or not disclose their  
7 PII/PHI to unauthorized third parties.

8           91. Defendant owed a duty of care to Plaintiff and Class members because it  
9 was foreseeable that Defendant’s failure—to use adequate data security in accordance  
10 with industry standards for data security—would compromise their PII/PHI in a data  
11 breach. And here, that foreseeable danger came to pass.

12           92. Defendant has full knowledge of the sensitivity of the PII/PHI and the types  
13 of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully  
14 disclosed.

15           93. Defendant owed these duties to Plaintiff and Class members because they  
16 are members of a well-defined, foreseeable, and probable class of individuals whom  
17 Defendant knew or should have known would suffer injury-in-fact from Defendant’s  
18 inadequate security practices. After all, Defendant actively sought and obtained Plaintiff  
19 and Class members’ PII/PHI.

20           94. Defendant owed—to Plaintiff and Class members—at least the following  
21 duties to:  
22

- 1 a. exercise reasonable care in handling and using the PII/PHI in its care
- 2 and custody;
- 3 b. implement industry-standard security procedures sufficient to
- 4 reasonably protect the information from a data breach, theft, and
- 5 unauthorized;
- 6 c. promptly detect attempts at unauthorized access;
- 7 d. notify Plaintiff and Class members within a reasonable timeframe of
- 8 any breach to the security of their PII/PHI.

9 95. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiff  
10 and Class members the scope, nature, and occurrence of the Data Breach. After all, this  
11 duty is required and necessary for Plaintiff and Class members to take appropriate  
12 measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm,  
13 and to take other necessary steps to mitigate the harm caused by the Data Breach.

14 96. Defendant also had a duty to exercise appropriate clearinghouse practices to  
15 remove PII/PHI it was no longer required to retain under applicable regulations.

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

20 98. Defendant's duty to use reasonable security measures arose because of the  
21 special relationship that existed between Defendant and Plaintiff and the Class. That  
22 special relationship arose because Plaintiff and the Class (or their third-party agents)



1 entrusted Defendant with their confidential PII/PHI, a necessary part of obtaining services  
2 from Defendant.

3 99. Under the FTC Act, 15 U.S.C. § 45, Defendant had a duty to use fair and  
4 adequate computer systems and data security practices to safeguard Plaintiff and Class  
5 members' PII/PHI.

6 100. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting  
7 commerce," including, as interpreted and enforced by the FTC, the unfair act or practice  
8 by businesses, such as Defendant, of failing to use reasonable measures to protect the  
9 PII/PHI entrusted to it. The FTC publications and orders promulgated pursuant to the FTC  
10 Act also form part of the basis of Defendant's duty to protect Plaintiff and the Class  
11 members' sensitive PII/PHI.

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

18 102. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards  
19 for privacy and security practices—as to protect Plaintiff's and Class members' PHI.

20 103. Defendant violated its duty under HIPAA by failing to use reasonable  
21 measures to protect its PHI and by not complying with applicable regulations detailed  
22 *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and  
23

1 amount of PHI that Defendant collected and stored and the foreseeable consequences of a  
2 data breach, including, specifically, the immense damages that would result to individuals  
3 in the event of a breach, which ultimately came to pass.

4 104. The risk that unauthorized persons would attempt to gain access to the  
5 PII/PHI and misuse it was foreseeable. Given that Defendant hold vast amounts of  
6 PII/PHI, it was inevitable that unauthorized individuals would attempt to access  
7 Defendant's databases containing the PII/PHI —whether by malware or otherwise.

8 105. PII/PHI is highly valuable, and Defendant knew, or should have known, the  
9 risk in obtaining, using, handling, emailing, and storing the PII/PHI of Plaintiff and Class  
10 members' and the importance of exercising reasonable care in handling it.

11 106. Defendant improperly and inadequately safeguarded the PII/PHI of Plaintiff  
12 and the Class in deviation of standard industry rules, regulations, and practices at the time  
13 of the Data Breach.

14 107. Defendant breached these duties as evidenced by the Data Breach.

15 108. Defendant acted with wanton and reckless disregard for the security and  
16 confidentiality of Plaintiff's and Class members' PII/PHI by:

- 17 a. disclosing and providing access to this information to third parties  
18 and  
19 b. failing to properly supervise both the way the PII/PHI was stored,  
20 used, and exchanged, and those in its employ who were responsible  
21 for making that happen.  
22  
23

1           109. Defendant breached its duties by failing to exercise reasonable care in  
2 supervising its agents, contractors, vendors, and suppliers, and in handling and securing  
3 the personal information and PII/PHI of Plaintiff and Class members which actually and  
4 proximately caused the Data Breach and Plaintiff and Class members' injury.

5           110. Defendant further breached its duties by failing to provide reasonably timely  
6 notice of the Data Breach to Plaintiff and Class members, which actually and proximately  
7 caused and exacerbated the harm from the Data Breach and Plaintiff and Class members'  
8 injuries-in-fact.

9           111. Defendant has admitted that the PII/PHI of Plaintiff and the Class was  
10 wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

11           112. As a direct and traceable result of Defendant's negligence and/or negligent  
12 supervision, Plaintiff and Class members have suffered or will suffer damages, including  
13 monetary damages, increased risk of future harm, embarrassment, humiliation, frustration,  
14 and emotional distress.

15           113. And, on information and belief, Plaintiff's PII/PHI has already been  
16 published—or will be published imminently—by cybercriminals on the Dark Web.

17           114. Defendant's breach of its common-law duties to exercise reasonable care  
18 and its failures and negligence actually and proximately caused Plaintiff and Class  
19 members actual, tangible, injury-in-fact and damages, including, without limitation, the  
20 theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of  
21 their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and  
22 remediate the effects of the Data Breach that resulted from and were caused by

1 Defendant's negligence, which injury-in-fact and damages are ongoing, imminent,  
2 immediate, and which they continue to face.

3 **SECOND CAUSE OF ACTION**  
4 **Breach of Implied Contract**  
5 **(On Behalf of Plaintiff and the Class)**

6 115. Plaintiff incorporates by reference all other paragraphs as if fully set forth  
7 herein.

8 116. Plaintiff and Class members either directly contracted with Defendant or  
9 Plaintiff and Class members were the third-party beneficiaries of contracts with  
10 Defendant.

11 117. Plaintiff and Class members (or their third-party agents) were required to  
12 provide their PII/PHI to Defendant as a condition of receiving products and/or services  
13 provided by Defendant. Plaintiff and Class members (or their third-party agents) provided  
14 their PII/PHI to Defendant or its third-party agents in exchange for Defendant's products  
15 and/or services.

16 118. The contracts entered into by Plaintiff's and Class members' agents (for  
17 example, their employers), were made for the direct benefit of Plaintiff and the Class.  
18 Specifically, Plaintiff's and Class members' third party agents entered into contracts with  
19 Defendant to products and/or services for Plaintiff and Class members.

20 119. Plaintiff and Class members (or their third-party agents) reasonably  
21 understood that a portion of the funds they paid Defendant would be used to pay for  
22 adequate cybersecurity measures.

1           120. Plaintiff and Class members (or their third-party agents) reasonably  
2 understood that Defendant would use adequate cybersecurity measures to protect the  
3 PII/PHI that they were required to provide based on Defendant's duties under state and  
4 federal law and its internal policies.

5           121. Plaintiff and the Class members (or their third-party agents) accepted  
6 Defendant's offers by disclosing their PII/PHI to Defendant or its third-party agents in  
7 exchange for products and/or services.

8           122. In turn, and through internal policies, Defendant agreed to protect and not  
9 disclose the PII/PHI to unauthorized persons.

10           123. Upon information and belief, in its Privacy Policy or other internal policies,  
11 Defendant represented that they had a legal duty to protect Plaintiff's and Class Member's  
12 PII/PHI.

13           124. Implicit in the parties' agreement was that Defendant would provide  
14 Plaintiff and Class members (or their third-party agents) with prompt and adequate notice  
15 of all unauthorized access and/or theft of their PII/PHI.

16           125. After all, Plaintiff and Class members (or their third-party agents) would not  
17 have entrusted their PII/PHI to Defendant (or their third-party agents) in the absence of  
18 such an agreement with Defendant.

19           126. Plaintiff and the Class (or their third-party agents) fully performed their  
20 obligations under the implied contracts with Defendant.

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

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

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

8 129. Defendant materially breached the contracts it entered with Plaintiff and  
9 Class members (or their third-party agents) by:

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

19 130. In these and other ways, Defendant violated its duty of good faith and fair  
20 dealing.

21 131. Defendant's material breaches were the direct and proximate cause of  
22 Plaintiff's and Class members' injuries (as detailed *supra*).

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

3 133. Plaintiff and Class members (or their third-party agents) performed as  
4 required under the relevant agreements, or such performance was waived by Defendant’s  
5 conduct.

6 **THIRD CAUSE OF ACTION**  
7 **Invasion of Privacy**  
8 **(On Behalf of Plaintiff and the Class)**

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

11 135. Plaintiff and the Class had a legitimate expectation of privacy regarding  
12 their highly sensitive and confidential PII/PHI and were accordingly entitled to the  
13 protection of this information against disclosure to unauthorized third parties.

14 136. Defendant owed a duty to its current and former consumers, including  
15 Plaintiff and the Class, to keep this information confidential.

16 137. The unauthorized acquisition (i.e., theft) by a third party of Plaintiff and  
17 Class members’ PII/PHI is highly offensive to a reasonable person.

18 138. The intrusion was into a place or thing which was private and entitled to be  
19 private. Plaintiff and the Class (or their third-party agents) disclosed their sensitive and  
20 confidential information to Defendant, but did so privately, with the intention that their  
21 information would be kept confidential and protected from unauthorized disclosure.  
22 Plaintiff and the Class were reasonable in their belief that such information would be kept  
23 private and would not be disclosed without their authorization.

1           139. The Data Breach constitutes an intentional interference with Plaintiff’s and  
2 the Class’s interest in solitude or seclusion, either as to their person or as to their private  
3 affairs or concerns, of a kind that would be highly offensive to a reasonable person.

4           140. Defendant acted with a knowing state of mind when it permitted the Data  
5 Breach because it knew its information security practices were inadequate.

6           141. Defendant acted with a knowing state of mind when it failed to notify  
7 Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially  
8 impairing their mitigation efforts.

9           142. Acting with knowledge, Defendant had notice and knew that its inadequate  
10 cybersecurity practices would cause injury to Plaintiff and the Class.

11           143. As a proximate result of Defendant’s acts and omissions, the private and  
12 sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now  
13 available for disclosure and redisclosure without authorization, causing Plaintiff and the  
14 Class to suffer damages (as detailed *supra*).

15           144. And, on information and belief, Plaintiff’s PII/PHI has already been  
16 published—or will be published imminently—by cybercriminals on the Dark Web.

17           145. Unless and until enjoined and restrained by order of this Court, Defendant’s  
18 wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the  
19 Class since their PII/PHI are still maintained by Defendant with their inadequate  
20 cybersecurity system and policies.

21           146. Plaintiff and the Class have no adequate remedy at law for the injuries  
22 relating to Defendant’s continued possession of their sensitive and confidential records. A  
23



1 judgment for monetary damages will not end Defendant's inability to safeguard the  
2 PII/PHI of Plaintiff and the Class.

3 147. In addition to injunctive relief, Plaintiff, on behalf of herself and the other  
4 Class members, also seeks compensatory damages for Defendant's invasion of privacy,  
5 which includes the value of the privacy interest invaded by Defendant, the costs of future  
6 monitoring of their credit history for identity theft and fraud, plus prejudgment interest  
7 and costs.

8 **FOURTH CAUSE OF ACTION**  
9 **Unjust Enrichment**  
10 **(On Behalf of Plaintiff and the Class)**

11 148. Plaintiff incorporates by reference all other paragraphs as if fully set forth  
12 herein.

13 149. This claim is pleaded in the alternative to the breach of implied contract  
14 claim.

15 150. Plaintiff and Class members (or their third-party agents) conferred a benefit  
16 upon Defendant. After all, Defendant benefitted from (1) their payment, and (2) using  
17 their PII/PHI to facilitate its provision of employee-benefit related products and/or  
18 services.

19 151. Defendant appreciated or had knowledge of the benefits it received from  
20 Plaintiff and Class members (or their third-party agents).

21 152. Plaintiff and Class members (or their third-party agents) reasonably  
22 understood that Defendant would use adequate cybersecurity measures to protect the  
23

1 PII/PHI that they were required to provide based on Defendant's duties under state and  
2 federal law and its internal policies.

3 153. Defendant enriched itself by saving the costs they reasonably should have  
4 expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

5 154. Instead of providing a reasonable level of security, or retention policies, that  
6 would have prevented the Data Breach, Defendant instead calculated to avoid its data  
7 security obligations at the expense of Plaintiff and Class members by utilizing cheaper,  
8 ineffective security measures. Plaintiff and Class members, on the other hand, suffered as  
9 a direct and proximate result of Defendant's failure to provide the requisite security.

10 155. Under principles of equity and good conscience, Defendant should not be  
11 permitted to retain the full value of Plaintiff's and Class members' (1) payment, and (2)  
12 PII/PHI because Defendant failed to adequately protect their PII/PHI.

13 156. Plaintiff and Class members have no adequate remedy at law.

14 157. Defendant should be compelled to disgorge into a common fund—for the  
15 benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it  
16 received because of its misconduct.

17 **FIFTH CAUSE OF ACTION**  
18 **Breach of Fiduciary Duty**  
**(On Behalf of Plaintiff and the Class)**

19 158. Plaintiff incorporates by reference all other paragraphs as if fully set forth  
20 herein.

21 159. Given the relationship between Defendant and Plaintiff and Class members,  
22 where Defendant became guardian of Plaintiff's and Class members' PII/PHI, Defendant

1 became a fiduciary by its undertaking and guardianship of the PII/PHI, to act primarily  
2 for Plaintiff and Class members, (1) for the safeguarding of Plaintiff and Class members'  
3 PII/PHI; (2) to timely notify Plaintiff and Class members of a Data Breach and disclosure;  
4 and (3) to maintain complete and accurate records of what information (and where)  
5 Defendant did and does store.

6 160. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class  
7 members upon matters within the scope of Defendant's relationship with them—  
8 especially to secure their PII/PHI.

9 161. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class  
10 members (or their third-party agents) would not have entrusted Defendant, or anyone in  
11 Defendant's position, to retain their PII/PHI had they known the reality of Defendant's  
12 inadequate data security practices.

13 162. Defendant breached its fiduciary duties to Plaintiff and Class members by  
14 failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

15 163. Defendant also breached its fiduciary duties to Plaintiff and Class members  
16 by failing to diligently discover, investigate, and give notice of the Data Breach in a  
17 reasonable and practicable period.

18 164. As a direct and proximate result of Defendant's breach of its fiduciary  
19 duties, Plaintiff and Class members have suffered and will continue to suffer numerous  
20 injuries (as detailed *supra*).

21 **SIXTH CAUSE OF ACTION**  
22 **Violation of the Arizona Consumer Fraud Act**  
23 **A.R.S. §§ 44-1521, *et seq.***

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

1  
2  
3 165. Plaintiff incorporates by reference all other paragraphs as if fully set forth  
4 herein.

5 166. Under A.R.S. § 44-1521, Defendant’s benefit-related products and services  
6 are “merchandise” because they are “objects, wares, goods, commodities, intangibles,  
7 real estate or services.”

8 167. The Arizona Consumer Fraud Act, A.R.S. § 44-1521, *et seq.*, prohibits:  
9 “[t]he act, use or employment by any person of any deception, deceptive or unfair act or  
10 practice, fraud, false pretense, false promise, misrepresentation, or concealment,  
11 suppression or omission of any material fact with intent that others rely on such  
12 concealment, suppression or omission, in connection with the sale or advertisement of any  
13 merchandise whether or not any person has in fact been misled, deceived or damaged  
14 thereby.”

15 168. Defendant violated the Arizona Consumer Fraud Act by engaging in  
16 deceptive and/or unfair acts or practices by:

- 17 a. failing to implement and maintain reasonable security and privacy  
18 measures to protect Plaintiff’s and Class members’ PII/PHI, which  
19 was a direct and proximate cause of the Data Breach;
- 20 b. failing to identify foreseeable security and privacy risks, remediate  
21 identified security and privacy risks, and adequately improve security  
22

1 and privacy measures following previous cybersecurity incidents,  
2 which was a direct and proximate cause of the Data Breach;

3 c. failing to comply with common law and statutory duties pertaining  
4 to the security and privacy of Plaintiff's and Class members' PII/PHI,  
5 including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA,  
6 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*, which  
7 was a direct and proximate cause of the Data Breach;

8 d. omitting, suppressing, and concealing the material fact that it did not  
9 reasonably or adequately secure Plaintiff's and Class members'  
10 PII/PHI; and

11 e. omitting, suppressing, and concealing the material fact that it did not  
12 comply with common law and statutory duties pertaining to the  
13 security and privacy of Plaintiff's and Class members' PII/PHI,  
14 including duties imposed by the FTC Act, 15 U.S.C. § 45, the FCRA,  
15 15 U.S.C. § 1681e, and the GLBA, 15 U.S.C. § 6801, *et seq.*

16 169. Defendant's omissions were material because they were likely to deceive  
17 reasonable consumers about the adequacy of Defendant's data security and ability to  
18 protect the confidentiality of their PII/PHI.

19 170. Defendant intended to mislead Plaintiff and Class members and induce them  
20 to rely on its omissions.

21 171. Had Defendant disclosed to Plaintiff and Class members (or their third-party  
22 agents) that its data systems were not secure—and thus vulnerable to attack—Defendant

1 would have been unable to continue in business and it would have been forced to adopt  
2 reasonable data security measures and comply with the law. Defendant accepted the  
3 PII/PHI that Plaintiff and Class members (or their third-party agents) entrusted to it while  
4 keeping the inadequate state of its security controls secret from the public. Accordingly,  
5 Plaintiff and Class members acted reasonably in relying on Defendant's omissions, the  
6 truth of which they could not have discovered through reasonable investigation.

7 172. Defendant acted intentionally, knowingly, maliciously, and recklessly  
8 disregarded Plaintiff's and Class members' rights.

9 173. As a direct and proximate result of Defendant's unfair and deceptive acts  
10 and practices, Plaintiff and Class members have suffered and will continue to suffer injury,  
11 ascertainable losses of money or property, and monetary and non-monetary damages,  
12 including from fraud and identity theft; time and expenses related to monitoring their  
13 financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity  
14 theft; and loss of value of their PII/PHI.

15 174. And, on information and belief, Plaintiff's PII/PHI has already been  
16 published—or will be published imminently—by cybercriminals on the Dark Web.

17 175. Plaintiff and Class members seek all monetary and non-monetary relief  
18 allowed by law.

19 **SEVENTH CAUSE OF ACTION**  
20 **Declaratory Judgment**  
**(On Behalf of Plaintiff and the Class)**

21 176. Plaintiff incorporates by reference all other paragraphs as if fully set forth  
22 herein.

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

5 178. In the fallout of the Data Breach, an actual controversy has arisen about  
6 Defendant’s various duties to use reasonable data security. On information and belief,  
7 Plaintiff alleges that Defendant’s actions were—and *still* are—inadequate and  
8 unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing  
9 threat of fraud and identity theft.

10 179. Given its authority under the Declaratory Judgment Act, this Court should  
11 enter a judgment declaring, among other things, the following:

- 12 a. Defendant owed—and continues to owe—a legal duty to use  
13 reasonable data security to secure the data entrusted to it;
- 14 b. Defendant has a duty to notify impacted individuals of the Data  
15 Breach under the common law and Section 5 of the FTC Act;
- 16 c. Defendant breached, and continues to breach, its duties by failing to  
17 use reasonable measures to the data entrusted to it; and
- 18 d. Defendant breaches of its duties caused—and continues to cause—  
19 injuries to Plaintiff and Class members.

20 180. The Court should also issue corresponding injunctive relief requiring  
21 Defendant to use adequate security consistent with industry standards to protect the data  
22 entrusted to it.

1 181. If an injunction is not issued, Plaintiff and the Class will suffer irreparable  
2 injury and lack an adequate legal remedy if Defendant experiences a second data breach.

3 182. And if a second breach occurs, Plaintiff and the Class will lack an adequate  
4 remedy at law because many of the resulting injuries are not readily quantified in full and  
5 they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put,  
6 monetary damages—while warranted for out-of-pocket damages and other legally  
7 quantifiable and provable damages—cannot cover the full extent of Plaintiff and Class  
8 members' injuries.

9 183. If an injunction is not issued, the resulting hardship to Plaintiff and Class  
10 members far exceeds the minimal hardship that Defendant could experience if an  
11 injunction is issued.

12 184. An injunction would benefit the public by preventing another data breach—  
13 thus preventing further injuries to Plaintiff, Class members, and the public at large.

14 **PRAYER FOR RELIEF**

15 Plaintiff and Class members respectfully request judgment against Defendant and  
16 that the Court enter an order:

- 17 A. Certifying this case as a class action on behalf of Plaintiff and the proposed  
18 Class, appointing Plaintiff as class representative, and appointing her  
19 counsel to represent the Class;
- 20 B. Awarding declaratory and other equitable relief as necessary to protect the  
21 interests of Plaintiff and the Class;
- 22



- 1 C. Awarding injunctive relief as necessary to protect the interests of Plaintiff  
2 and the Class;
- 3 D. Enjoining Defendant from further unfair and/or deceptive practices;
- 4 E. Awarding Plaintiff and the Class damages including applicable  
5 compensatory, exemplary, punitive damages, and statutory damages, as  
6 allowed by law;
- 7 F. Awarding restitution and damages to Plaintiff and the Class in an amount to  
8 be determined at trial;
- 9 G. Awarding attorneys' fees and costs, as allowed by law;
- 10 H. Awarding prejudgment and post-judgment interest, as provided by law;
- 11 I. Granting Plaintiff and the Class leave to amend this complaint to conform  
12 to the evidence produced at trial; and
- 13 J. Granting other relief that this Court finds appropriate.
- 14

15 **DEMAND FOR JURY TRIAL**

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

17 Date: August 28, 2024

18 Respectfully submitted,

19 By: /s/ Andrew J. Shamis

20 Andrew J. Shamis (AZ Bar No. 037343)

21 **SHAMIS & GENTILE, P.A.**

22 14 NE 1st Ave, Suite 705

Miami, FL 33132

23 Tel: (305) 479-2299

Email: ashamis@shamisgentile.com

/s/ Samuel Strauss

Samuel J. Strauss\*

Raina C. Borrelli\*

**STRAUSS BORRELLI PLLC**

980 N. Michigan Avenue, Suite 1610

Chicago, Illinois 60611

T: (872) 263-1100

F: (872) 263-1109

sam@straussborrelli.com

raina@straussborrelli.com

*\*Pro hac vice forthcoming*

*Attorneys for Plaintiff and Proposed Class*

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Employee Benefits Enrollment Platform Enroll Confidentially Facing Class Action Over February 2024 Data Breach](#)

---