IN THE CIRCUIT COURT OF THE FIFTEENTH JUDICIAL CIRCUIT IN AND FOR PALM BEACH COUNTY, FLORIDA

EMILY BENNETT, on behalf of herself and all others similarly situated, Plaintiff, v. **HOLISTIX TREATMENT CENTERS, LLC d/b/a LAKE WORTH HOLISTIX DETOX d/b/a LEVEL UP TREATMENT LAKE WORTH,** Defendant.	No. **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Emily Bennett ("Plaintiff"), through her attorneys, individually and on behalf of all others similarly situated, brings this Class Action Complaint against Defendant Holistix Treatment Centers, LLC d/b/a Lake Worth Holistix Detox d/b/a Level Up Treatment Lake Worth ("Level Up" 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. This class action arises from Level Up's failure to protect highly sensitive data.

2. Level Up is an addiction treatment facility focused on providing behavioral healthcare management and treatment to individuals "from all around the United States, Canada, and internationally."[1]

3. As such, Level Up stores a litany of highly sensitive personal identifiable information ("PII") and protected health information ("PHI") (collectively "PII/PHI") about its current and former patients. But Level Up lost control over that data when cybercriminals infiltrated its insufficiently protected computer systems in a data breach (the "Data Breach").

4. Upon information and belief, the Data Breach impacted at least 6,567 individuals.[2] Upon information and belief, the victims of the Data Breach included Defendant's current and former patients.

5. According to Defendant's Breach Notice, on or about July 26, 2024, Defendant discovered that it was the target of a cyberattack. In other words, Level Up had no effective means to prevent, detect, stop, or mitigate breaches of its systems—thereby allowing cybercriminals unrestricted access to its current and former patients' PII/PHI.

6. On information and belief, cybercriminals were able to breach Level Up's systems because Level Up failed to adequately train its employees on cybersecurity and failed to maintain reasonable security safeguards or protocols to protect the Class's PII/PHI. In short, Level Up's failures placed the Class's PHI in a vulnerable position—rendering them easy targets for cybercriminals.

[1] About, Level Up Lake Worth, https://leveluplakeworth.com/about/ (last visited October 10, 2024).
[2] Breach Portal Notice to Secretary of HHS Breach of Unsecured Protected Health Information, U.S. Dept. of Health and Human Services, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (last visited October 11, 2024).

7. Plaintiff is a Data Breach victim, having received a breach notice—a copy of Plaintiff's Breach Notice is attached as Exhibit A. She brings this class action on behalf of herself, and all others harmed by Level Up's misconduct.

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

PARTIES

9. Plaintiff, Emily Bennett, is a natural person and citizen of Pennsylvania. She resides in Kane, Pennsylvania where she intends to remain.

10. Defendant, Holistix Treatment Centers, LLC d/b/a Lake Worth Holistix Detox d/b/a Level Up Treatment Lake Worth is a Florida Limited Liability Company with its principal place of business at 9935 Palomino Drive, Lake Worth, Florida 33467, Palm Beach County.

JURISDICTION AND VENUE

11. This Court has subject matter jurisdiction over Plaintiffs' claims under Florida Stat. § 26.012 and § 86.011. This Court has jurisdiction over this dispute because this complaint seeks damages in excess of $50,000.00, exclusive of interest and attorneys' fees.

12. This Court has personal jurisdiction over Defendant because under Florida Stat. §48.193, Defendant personally or through their agents operated, conducted, engaged in, or carried on a business or business venture in Florida and/or had offices in Florida committed tortious acts in Florida, and because Defendant engaged in significant business activity within Florida.

13. Venue is proper Palm Beach County pursuant to Florida Stat. § 47.011 and § 47.051 because Defendant is headquartered and does business in this county, the cause of action accrued

in this county, and Defendant has an office for the transaction of its customary business in this county.

BACKGROUND

Level Up Collected and Stored the PII/PHI of Plaintiff and the Class

14. Level Up is an addiction treatment and recovery center headquartered in Lake Worth, Florida.[3]

15. As part of its business, Level Up receives and maintains the PII/PHI of thousands of its current and former patients.

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

17. Under state and federal law, businesses like Level Up have duties to protect its current and former patients' PII/PHI and to notify them about breaches.

18. Level Up recognizes these duties, declaring in its "Privacy Policy" that:

a. "We are committed to protecting your privacy;"

b. "We pledge to obtain your consent before collecting your personal information and to safeguard any personal information you provide;"

c. "We take necessary security measures to protect against unauthorized access to or unauthorized alteration, disclosure, or destruction of data. These include internal reviews of our data collection, storage, and processing practices, and security measures, including data encryption, and

[3] About, LinkedIn, https://www.linkedin.com/showcase/level-up-lake-worth/about/ (last visited October 11, 2024).

administrative and physical security measures to guard against unauthorized access to systems where we store personal data;"

d. "We restrict access to personal including protected health information to We Level Up employees, contractors, and agents who need to know that information to provide you with the services you are seeking out on our behalf."[4]

Level Up's Data Breach

19. On or about July 26, 2024, Defendant discovered that an unauthorized actor had gained access to Level Up's systems resulting in the exposure of current and former patients' information, including their first and last names, mailing addresses, Social Security numbers, and protected health information.[5]

20. Due to the obfuscating nature of Defendant's Breach Notice, it is unclear how long cybercriminals had an unfettered access to peruse and exfiltrate PII/PHI before being detected.

21. Because of Level Up's Data Breach, at least the following types of PII/PHI were compromised:

a. name;

b. Social Security number;

c. mailing address; and

d. protected health information.[6]

[4] Privacy Policy, Level Up Lake Worth, https://weleveluppalmbeach.com/privacy-policy/ (last visited October 11, 2024).
[5] Notice of Data Security Incident, Level Up Lake Worth, https://leveluplakeworth.com/notice-of-data-security-incident/ (last visited October 11, 2024).
[6] *Id.*

22. And yet, Level Up waited until September 27, 2024, before it began notifying the class—two months after it discovered the Data Breach. Ex. A.

23. Thus, Level Up kept the Class in the dark—thereby depriving the Class of the opportunity to try and mitigate their injuries in a timely manner.

24. And when Level Up did notify Plaintiff and the Class of the Data Breach, Level Up acknowledged that the Data Breach created a present, continuing, and significant risk of suffering identity theft, encouraging Plaintiff and the Class to:

a. "remain vigilant to protect against fraud and/or identity theft by, among other things, reviewing their financial account statements and monitoring free credit reports;"

b. "promptly notify the institution or company with which the account is maintained [if individuals detect any suspicious activity on an account];"

c. "promptly report any fraudulent activity or any suspected identity theft to proper law enforcement authorities;" and

d. "review the tips provided by the Federal Trade Commission ("FTC") on fraud alerts, free security/credit freezes and steps that they can take to avoid identity theft."[7]

25. Level Up also acknowledged the risks associated with stolen PII/PHI, encouraging victims to protect themselves in the following ways:

a. "enroll in credit monitoring services;"

b. "place a security freeze on your credit reports;"

c. "place a fraud alert on your credit file;" and

[7] *Id.*

d. "review your credit reports and your credit card and other financial accounts for any unauthorized activity." Ex A.

26. Level Up failed its duties when its inadequate security practices caused the Data Breach. In other words, Level Up's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII/PHI. And thus, Level Up caused widespread injury and monetary damages.

27. Since the breach, Level Up has declared that it is "implementing additional safeguards and enhanced security measures to better protect the privacy and security of information in its systems." Ex. A. But this is too little too late. Simply put, these measures—which Level Up now recognizes as necessary—should have been implemented *before* the Data Breach.

28. On information and belief, Level Up failed to adequately train its employees on reasonable cybersecurity protocols or implement reasonable security measures.

29. It is unknown how many individuals were impacted by the Data Breach, however upon information and belief, the victims include Level Up's current and former patients.

30. Further, the Notice of Data Breach shows that Level Up cannot—or will not—determine the full scope of the Data Breach, as Level Up has been unable to determine precisely when the cybercriminals gained access to its systems, how long they had access, how the breach occurred, and why it took them a year to notified affected individuals.

31. Level Up has done little to remedy its Data Breach. Level Up has offered victims credit monitoring and identity related services. However, such services are wholly insufficient to compensate Plaintiff and Class members for the injuries that Level Up inflicted upon them.

32. Because of Level Up's Data Breach, the PII/PHI of Plaintiff and Class members was placed into the hands of cybercriminals—inflicting numerous injuries and significant damages upon Plaintiff and Class members.

33. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[8]

34. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's Private Information. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

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

RansomHub claims credit—and threatens to publish PII/PHI

36. Worryingly, the cybercriminals that obtained Plaintiff's and Class members' PII/PHI appear to be the notorious Ransomware group "RansomHub."[9]

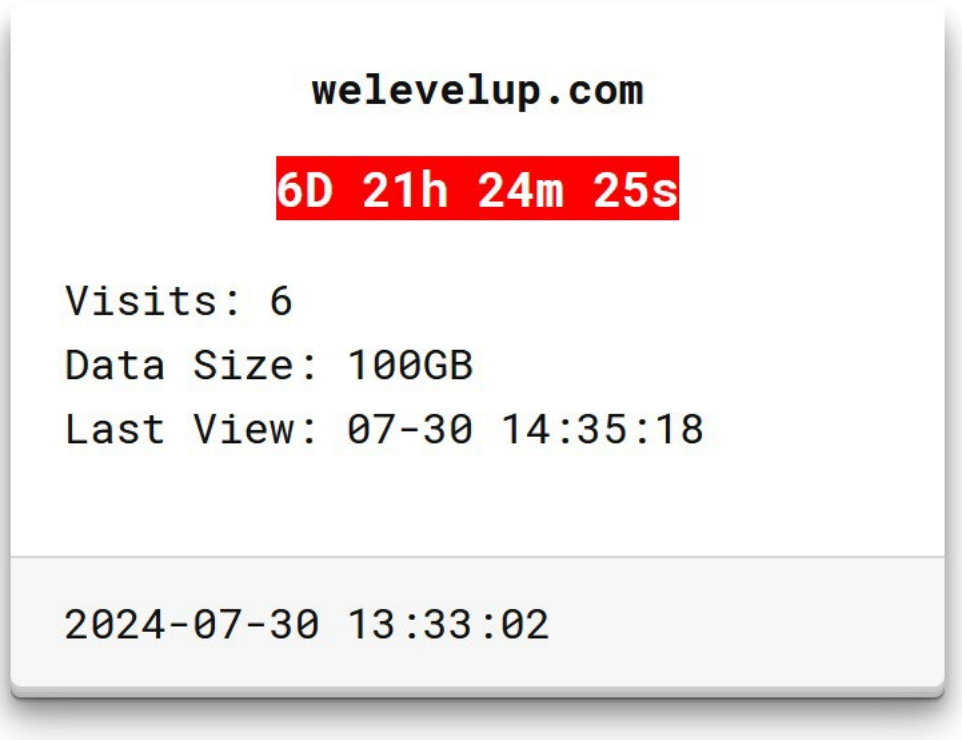
37. On July 30, 2024, RansomHub claimed credit for the Data Breach on its Dark Web website.[10]

---

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

[9] RansomHub Ransomware Attack Exposes 100GB of We Level Up Data, Halcyon, https://ransomwareattacks.halcyon.ai/attacks/ransomhub-ransomware-attack-exposes-100gb-of-we-level-up-data (last visited October 11, 2024).

[10] *Id.*; *See e.g.,* @FalconFeedsio, Twitter (X) (July 30, 2024, 10:06 AM), *https://x.com/FalconFeedsio/status/1818302051962720365/photo/1*.



38. Thereafter, RansomHub set a deadline for August 6, 2024 and indicated that it would *publish* the stolen PII/PHI unless a ransom was paid.[11]

39. Thus, it appears Plaintiff's and Class members' PII was *already published* on the Dark Web—given that the August 2024 deadline has long since passed.

40. RansomHub is a new emergence in the cyber threat landscape and is believed to "have roots in Russia and operates as a Ransomware-as-a-Service (RaaS) group."[12] RansomHub "distinguishes itself by making claims and backing them up with data leaks."[13]

41. And as the Harvard Business Review notes, such "[c]ybercriminals frequently use the Dark Web—a hub of criminal and illicit activity—to sell data from companies that they have

[11] *Id.*
[12] *Id.*
[13] *Id.*

gained unauthorized access to through credential stuffing attacks, phishing attacks, [or] hacking."[14]

42. Thus, on information and belief, Plaintiff's and the Class's stolen PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

Plaintiff's Experiences and Injuries

43. Plaintiff Emily Bennett is a former patient of Level Up, having received services from Level Up between October and November 2022.

44. Thus, Level Up obtained and maintained Plaintiff's PII/PHI.

45. As a result, Plaintiff was injured by Level Up's Data Breach.

46. As a condition of receiving services with Defendant, Plaintiff provided Level Up with her PII/PHI and allowed them to maintain her PII/PHI. Level Up used her PII/PHI to facilitate its services.

47. Plaintiff trusted the company would use reasonable measures to protect her PII/PHI according to Level Up's internal policies, as well as state and federal law. Level Up obtained and continues to maintain Plaintiff's PII/PHI and has a continuing legal duty and obligation to protect that PII/PHI from unauthorized access and disclosure.

48. Plaintiff reasonably understood that a portion of the funds she paid for services would be used to pay for adequate cybersecurity and protection of PII/PHI.

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

50. Plaintiff received a Notice of Data Breach from Defendant.

---

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

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

52. Through its Data Breach, Level Up compromised Plaintiff's:

a. full name;

b. mailing address;

c. Social Security number;

d. protected health information. Ex. A.

53. Plaintiff has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from medical identity theft. After all, Level Up directed Plaintiff to take those steps in its breach notice.

54. Plaintiff fears for the security of her PII/PHI and worries about what information was exposed in the Data Breach.

55. Because of Level Up's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

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

57. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and medical identity theft—all because Level Up's Data Breach placed Plaintiff's PII/PHI right in the hands of criminals.

58. Indeed, following the Data Breach, Plaintiff began experiencing a substantial increase in spam and scam phone calls, suggesting that her PII/PHI has already been placed in the hands of cybercriminals.

59. On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach, as cybercriminals are able to use an individual's PII that is accessible on the dark web, as Plaintiff's is here, to gather and steal even more information.

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

61. Today, Plaintiff has a continuing interest in ensuring that her PII/PHI—which, upon information and belief, remains backed up in Level Up's possession—is protected and safeguarded from additional breaches.

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

62. Because of Level Up's failure to prevent the Data Breach, Plaintiff and Class members suffered—and will continue to suffer—damages. These damages include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress. Also, they suffered or are at an increased risk of suffering:

a. loss of the opportunity to control how their PII/PHI is used;

b. diminution in value of their PII/PHI;

c. compromise and continuing publication of their PII/PHI;

d. out-of-pocket costs from trying to prevent, detect, and recovery from identity theft and fraud;

e. lost opportunity costs and wages from spending time trying to mitigate the fallout of the Data Breach by, *inter alia*, preventing, detecting, contesting, and recovering from identify theft and fraud;

f. delay in receipt of tax refund monies;

g. unauthorized use of their stolen PII/PHI; and

h. continued risk to their PII/PHI—which remains in Level Up's possession—and is thus as risk for futures breaches so long as Level Up fails to take appropriate measures to protect the PII/PHI.

63. Stolen PII/PHI is one of the most valuable commodities on the criminal information black market.

64. According to the National Association of Healthcare Access Management, "[p]ersonal medical data is said to be more than ten times as valuable as credit card information. PHI has such a high value because it contains highly sensitive information, such as social security numbers, birth dates, addresses, credit card numbers, telephone numbers and medical conditions. This data is incredibly valuable on the black market because, unlike a stolen credit card that can be easily canceled, most people are unaware that their medical information has been stolen."[15]

65. According to Advent Health University, when an electronic health record "lands in the hands of nefarious persons the results can range from fraud to identity theft to extortion. In fact, these records provide such valuable information that hackers can sell a single stolen medical record for up to $1,000."[16]

[15] https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information#:~:text=Personal%20medical%20data%20is%20said,telephone%20numbers%20and%20medical%20conditions, (last visited October 10, 2024).
[16] https://www.ahu.edu/blog/data-security-in-healthcare (last visited October 10, 2024).

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

67. Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase Private Information on the black market for the purpose of target-marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

68. According to an article in the HIPAA Journal posted on October 14, 2022, cybercriminals hack into medical practices for their "highly prized" medical records. "[T]he number of data breaches reported by HIPAA-regulated entities continues to increase every year. 2021 saw 714 data breaches of 500 or more records reported to the [HHS' Office for Civil Rights] OCR – an 11% increase from the previous year. Almost three-quarters of those breaches were classified as hacking/IT incidents."[17]

69. Healthcare organizations are easy targets because "even relatively small healthcare providers may store the records of hundreds of thousands of patients. The stored data is highly detailed, including demographic data, Social Security numbers, financial information, health insurance information, and medical and clinical data, and that information can be easily monetized."[18]

70. The HIPAA Journal article goes on to explain that patient records, like those stolen from Level Up, are "often processed and packaged with other illegally obtained data to create full record sets (the previously mentioned Fullz package) that contain extensive information on

[17] https://www.hipaajournal.com/why-do-criminals-target-medical-records/ (last visited October 10, 2024).
[18] *Id.*

individuals, often in intimate detail." The record sets are then sold on dark web sites to other criminals and "allows an identity kit to be created, which can then be sold for considerable profit to identity thieves or other criminals to support an extensive range of criminal activities."[19]

71. Data breaches such as the one experienced by Defendant have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, can prepare for, and hopefully can ward off a potential attack.

72. In fact, according to the cybersecurity firm Mimecast, 90% of healthcare organizations experienced cyberattacks in the past year.[20]

73. These significant increases in attacks to companies, particularly those in the healthcare industry, and attendant risk of future attacks, is widely known to the public and to anyone in that industry, including Defendant Level Up.

74. A study by Experian found that the average total cost of medical identity theft is "nearly $13,500" per incident, and that many victims were forced to pay out-of-pocket costs for fraudulent medical care.[21] Victims of healthcare data breaches often find themselves "being denied care, coverage or reimbursement by their medical insurers, having their policies canceled or having to pay to reinstate their insurance, along with suffering damage to their credit ratings and scores."[22]

75. Moreover, there may be a time lag between when harm occurs versus when it is discovered, and also between when Private Information is stolen and when it is used. According

[19] *Id.*
[20] https://www.securitymagazine.com/articles/93988-iowa-city-hospital-suffers-phishing-attack (last visited October 10, 2024).
[21] https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last visited October 10, 2024).
[22] *Id.*

to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

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

76. It is incorrect to assume that reimbursing a victim for a financial loss due to fraud makes that individual whole again. Similar to the GAO's study, the Department of Justice's Bureau of Justice Statistics ("BJS") found that "among victims who had personal information used for fraudulent purposes, about a third (32%) spent a month or more resolving problems."[23] In fact, the BJS reported, "resolving the problems caused by identity theft [could] take more than a year for some victims."[24]

77. Further, once a patient's medical information is in the hands of thieves, they have access to the individual's health insurance and may use it to obtain free medical care, which can "ruin credit and take months, or even years, to resolve."[25]

78. As the fraudulent activity resulting from the Data Breach may not come to light for years, Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

Level Up Knew—Or Should Have Known—of the Risk of a Data Breach

[23] https://bjs.ojp.gov/content/pub/pdf/vit14.pdf (last visited October 10, 2024).
[24] *Id.*
[25] https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information#:~:text=Personal%20medical%20data%20is%20said,telephone%20numbers%20and%20medical%20conditions (last visited October 10, 2024).

79. Level Up's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years.

80. In 2021, a record 1,862 data breaches occurred, exposing approximately 293,927,708 sensitive records—a 68% increase from 2020.[26]

81. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service issue warnings to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals . . . because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[27]

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

Level Up Failed to Follow FTC Guidelines

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

---

[26] *See 2021 Data Breach Annual Report*, IDENTITY THEFT RESOURCE CENTER (Jan. 2022) https://notified.idtheftcenter.org/s/.

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

84. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*. There, the FTC set guidelines for what data security principles and practices businesses must use.[28] The FTC declared that, *inter alia*, businesses must:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

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

86. Furthermore, the FTC explains that companies must:

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

b. limit access to sensitive data;

c. require complex passwords to be used on networks;

d. use industry-tested methods for security;

e. monitor for suspicious activity on the network; and

f. verify that third-party service providers use reasonable security measures.

87. The FTC brings enforcement actions against businesses for failing to protect customer data adequately and reasonably. Thus, the FTC treats the failure—to use reasonable and appropriate measures to protect against unauthorized access to confidential consumer data—as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15

[28] *Protecting Personal Information: A Guide for Business,* FEDERAL TRADE COMMISSION (Oct. 2016) https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

88. In short, Level Up's failure to use reasonable and appropriate measures to protect against unauthorized access to its current and former patients' data constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Level Up Failed to Follow Industry Standards

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

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

91. Upon information and belief, Level Up failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

92. These frameworks are applicable and accepted industry standards. And by failing to comply with these accepted standards, Level Up opened the door to the criminals—thereby causing the Data Breach.

Level Up Violated HIPAA

93. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep patients' medical information safe. HIPAA compliance provisions, commonly known as the Administrative Simplification Rules, establish national standards for electronic transactions and code sets to maintain the privacy and security of protected health information.[29]

94. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of PHI and PHI is properly maintained.[30]

95. The Data Breach itself resulted from a combination of inadequacies showing Level Up failed to comply with safeguards mandated by HIPAA. Level Up's security failures include, but are not limited to:

a. failing to ensure the confidentiality and integrity of electronic PHI that it creates, receives, maintains and transmits in violation of 45 C.F.R. § 164.306(a)(1);

[29] HIPAA lists 18 types of information that qualify as PHI according to guidance from the Department of Health and Human Services Office for Civil Rights, and includes, *inter alia*: names, addresses, any dates including dates of birth, Social Security numbers, and medical record numbers.

[30] *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).

b. failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

c. failing to protect against any reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules regarding individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

d. failing to ensure compliance with HIPAA security standards by Level Up's workforce in violation of 45 C.F.R. § 164.306(a)(4);

e. failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

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

g. failing to identify and respond to suspected or known security incidents and failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity in violation of 45 C.F.R. § 164.308(a)(6)(ii);

h. failing to effectively train all staff members on the policies and procedures with respect to PHI as necessary and appropriate for staff members to carry out their functions and to maintain security of PHI in violation of 45 C.F.R. § 164.530(b) and 45 C.F.R. § 164.308(a)(5); and

i. failing to design, implement, and enforce policies and procedures establishing physical and administrative safeguards to reasonably safeguard PHI, in compliance with 45 C.F.R. § 164.530(c).

96. Simply put, the Data Breach resulted from a combination of insufficiencies that demonstrate Level Up failed to comply with safeguards mandated by HIPAA regulations.

CLASS ACTION ALLEGATIONS

97. Plaintiff brings this class action on behalf of herself and a proposed class of similarly situated individuals under Florida Rule of Civil Procedure 1.220 preliminarily defined as (the "Class"):

> All individuals residing in the United States whose PII/PHI was compromised in the Data Breach discovered by Level Up in July 2024, including all those individuals who received notice of the breach.

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

99. Plaintiff reserves the right to amend the class definition.

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

101. Ascertainability. All members of the proposed Class are readily ascertainable from information in Level Up's custody and control. After all, Level Up already identified some individuals and sent them data breach notices.

102. Numerosity. The Class members are so numerous that joinder of all Class members is impracticable. Upon information and belief, the proposed Class includes at 6567 members.

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

104. Adequacy. Plaintiff will fairly and adequately protect the proposed Class's common interests. Her interests do not conflict with Class members' interests. And Plaintiff has retained counsel—including lead counsel—that is experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf.

105. Commonality and Predominance. Plaintiff's and the Class's claims raise predominantly common fact and legal questions—which predominate over any questions affecting individual Class members—for which a class wide proceeding can answer for all Class members. In fact, a class wide proceeding is necessary to answer the following questions:

a. if Level Up had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII/PHI;

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

c. if Level Up were negligent in maintaining, protecting, and securing PII/PHI;

d. if Level Up breached contract promises to safeguard Plaintiff and the Class's PII/PHI;

e. if Level Up took reasonable measures to determine the extent of the Data Breach after discovering it;

f. if Level Up's Breach Notice was reasonable;

g. if the Data Breach caused Plaintiff and the Class injuries;

h. what the proper damages measure is; and

i. if Plaintiff and the Class are entitled to damages, treble damages, and or injunctive relief.

106. The Class also satisfies the criteria for certification under Florida Rule of Civil Procedure 1.220(b). Among other things, Plaintiffs aver that the prosecution of separate actions by the individual members of the proposed Class would create a risk of inconsistent or varying adjudication which would establish incompatible standards of conduct for Defendant; that the prosecution of separate actions by individual class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests; that Defendant has acted or refused to act on grounds that apply generally to the proposed Class, thereby making final injunctive relief or declaratory relief described herein appropriate with respect to the proposed Class as a whole; that questions of law or fact common to the Class predominate over any questions affecting only individual members and that class action treatment is superior to other available methods for the fair and efficient adjudication of the controversy which is the subject of this action. Plaintiffs further state that the interests of judicial economy will be served by concentrating litigation concerning these claims in this Court, and that the management of the Class will not be difficult.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiff and the Class)

107. Plaintiff incorporates by reference paragraphs 1–99 as if fully set forth herein.

108. Plaintiff and the Class entrusted their PII/PHI to Level Up on the premise and with the understanding that Level Up would safeguard their PII/PHI, use their PHI to provide services only, and/or not disclose their PII/PHI to unauthorized third parties.

109. Level Up owed a duty of care to Plaintiff and Class members because it was foreseeable that Level Up's failure—to use adequate data security in accordance with industry standards for data security—would compromise their PII/PHI in a data breach. And here, that foreseeable danger came to pass.

110. Level Up has full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and the Class could and would suffer if their PII/PHI was wrongfully disclosed.

111. Level Up owed these duties to Plaintiff and Class members because they are members of a well-defined, foreseeable, and probable class of individuals whom Level Up knew or should have known would suffer injury-in-fact from Level Up's inadequate security practices. After all, Level Up actively sought and obtained Plaintiff and Class members' PII/PHI.

112. Level Up owed—to Plaintiff and Class members—at least the following duties to:

a. exercise reasonable care in handling and using the PII/PHI in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiff and Class members within a reasonable timeframe of any breach to the security of their PII/PHI.

113. Thus, Level Up owed a duty to timely and accurately disclose to Plaintiff and Class members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and

necessary for Plaintiff and Class members to take appropriate measures to protect their PII/PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

114. Level Up also had a duty to exercise appropriate clearinghouse practices to remove PII/PHI it was no longer required to retain under applicable regulations.

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

116. Level Up's duty to use reasonable security measures arose because of the special relationship that existed between Level Up and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Level Up with their confidential PII/PHI, a necessary part of obtaining services from Defendant.

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

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

119. Level Up violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect PII/PHI and not complying with applicable industry standards as described in detail herein. Level Up's conduct was particularly unreasonable given the nature and

amount of PII/PHI Level Up had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

120. Similarly, under HIPAA, Level Up had a duty to follow HIPAA standards for privacy and security practices—as to protect Plaintiff's and Class members' PII/PHI.

121. Level Up violated its duty under HIPAA by failing to use reasonable measures to protect its PII/PHI and by not complying with applicable regulations detailed *supra*. Here too, Level Up's conduct was particularly unreasonable given the nature and amount of PII/PHI that Level Up collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

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

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

124. Level Up improperly and inadequately safeguarded the PII/PHI of Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

125. Level Up breached these duties as evidenced by the Data Breach.

126. Level Up acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and Class members' PII/PHI by:

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

b. failing to properly supervise both the way the PII/PHI was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

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

128. Level Up further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and Class members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff and Class members' injuries-in-fact.

129. Level Up has admitted that the PII/PHI of Plaintiff and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

130. As a direct and traceable result of Level Up's negligence and/or negligent supervision, Plaintiff and Class members have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

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

132. Level Up's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and Class members actual,

tangible, injury-in-fact and damages, including, without limitation, the theft of their PII/PHI by criminals, improper disclosure of their PII/PHI, lost benefit of their bargain, lost value of their PII/PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Level Up's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

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

133. Plaintiff incorporates by reference paragraphs 1–99 as if fully set forth herein.

134. Plaintiff and Class members were required to provide their PII/PHI to Level Up as a condition of receiving services provided by Defendant. Plaintiff and Class members provided their PII/PHI to Level Up in exchange for Level Up's services.

135. Plaintiff and Class members reasonably understood that a portion of the funds they paid Level Up would be used to pay for adequate cybersecurity measures.

136. Plaintiff and Class members reasonably understood that Level Up would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Level Up's duties under state and federal law and its internal policies.

137. Plaintiff and the Class members accepted Level Up's offers by disclosing their PII/PHI to Level Up in exchange for services.

138. In turn, and through internal policies, Level Up agreed to protect and not disclose the PII/PHI to unauthorized persons.

139. In its Privacy Policy, Level Up represented that they had a legal duty to protect Plaintiff's and Class Member's PII/PHI.

140. Implicit in the parties' agreement was that Level Up would provide Plaintiff and Class members with prompt and adequate notice of all unauthorized access and/or theft of their PII/PHI.

141. After all, Plaintiff and Class members would not have entrusted their PII/PHI to Level Up in the absence of such an agreement with Defendant.

142. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendant.

143. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

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

145. Level Up materially breached the contracts it entered with Plaintiff and Class members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information.

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII/PHI that Level Up created, received, maintained, and transmitted.

146. In these and other ways, Level Up violated its duty of good faith and fair dealing.

147. Level Up's material breaches were the direct and proximate cause of Plaintiff's and Class members' injuries (as detailed *supra*).

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

149. Plaintiff and Class members performed as required under the relevant agreements, or such performance was waived by Level Up's conduct.

THIRD CAUSE OF ACTION
Invasion of Privacy
(On Behalf of Plaintiff and the Class)

150. Plaintiff incorporates by reference paragraphs 1–99 as if fully set forth herein.

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

152. Level Up owed a duty to its current and former patients, including Plaintiff and the Class, to keep this information confidential.

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

154. The intrusion was into a place or thing which was private and entitled to be private. Plaintiff and the Class disclosed their sensitive and confidential information to Defendant, but did

so privately, with the intention that their information would be kept confidential and protected from unauthorized disclosure. Plaintiff and the Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

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

156. Level Up acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

157. Level Up acted with a knowing state of mind when it failed to notify Plaintiff and the Class in a timely fashion about the Data Breach, thereby materially impairing their mitigation efforts.

158. Acting with knowledge, Level Up had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

159. As a proximate result of Level Up's acts and omissions, the private and sensitive PII/PHI of Plaintiff and the Class were stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages (as detailed *supra*).

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

161. Unless and until enjoined and restrained by order of this Court, Level Up's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII/PHI are still maintained by Level Up with their inadequate cybersecurity system and policies.

162. Plaintiff and the Class have no adequate remedy at law for the injuries relating to Level Up's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Level Up's inability to safeguard the PII/PHI of Plaintiff and the Class.

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

FOURTH CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

164. Plaintiff incorporates by reference paragraphs 1–99 as if fully set forth herein.

165. This claim is pleaded in the alternative to the breach of implied contract claim.

166. Plaintiff and Class members conferred a benefit upon Defendant. After all, Level Up benefitted from using their PII/PHI to provide services and benefitted from the payment provided in exchange for services.

167. Level Up appreciated or had knowledge of the benefits it received from Plaintiff and Class members.

168. Plaintiff and Class members reasonably understood that Level Up would use adequate cybersecurity measures to protect the PII/PHI that they were required to provide based on Level Up's duties under state and federal law and its internal policies.

169. Level Up enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiff's and Class members' PII/PHI.

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

171. Under principles of equity and good conscience, Level Up should not be permitted to retain the full value of Plaintiff's and Class members' payment because Level Up failed to adequately protect their PII/PHI.

172. Plaintiff and Class members have no adequate remedy at law.

173. Level Up should be compelled to disgorge into a common fund—for the benefit of Plaintiff and Class members—all unlawful or inequitable proceeds that it received because of its misconduct.

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

174. Plaintiff incorporates by reference paragraphs 1–99 as if fully set forth herein.

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

176. Level Up has a fiduciary duty to act for the benefit of Plaintiff and Class members upon matters within the scope of Level Up's relationship with them—especially to secure their PII/PHI.

177. Because of the highly sensitive nature of the PII/PHI, Plaintiff and Class members would not have entrusted Defendant, or anyone in Level Up's position, to retain their PII/PHI had they known the reality of Level Up's inadequate data security practices.

178. Level Up breached its fiduciary duties to Plaintiff and Class members by failing to sufficiently encrypt or otherwise protect Plaintiff's and Class members' PII/PHI.

179. Level Up also breached its fiduciary duties to Plaintiff and Class members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period.

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

SIXTH CAUSE OF ACTION
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

181. Plaintiff incorporates by reference paragraphs 1–99 as if fully set forth herein.

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

183. In the fallout of the Data Breach, an actual controversy has arisen about Level Up's various duties to use reasonable data security. On information and belief, Plaintiff alleges that

Level Up's actions were—and *still* are—inadequate and unreasonable. And Plaintiff and Class members continue to suffer injury from the ongoing threat of fraud and identity theft.

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

a. Level Up owed—and continues to owe—a legal duty to use reasonable data security to secure the data entrusted to it;

b. Level Up has a duty to notify impacted individuals of the Data Breach under the common law and Section 5 of the FTC Act;

c. Level Up breached, and continues to breach, its duties by failing to use reasonable measures to the data entrusted to it; and

d. Level Up breaches of its duties caused—and continues to cause—injuries to Plaintiff and Class members.

185. The Court should also issue corresponding injunctive relief requiring Level Up to use adequate security consistent with industry standards to protect the data entrusted to it.

186. If an injunction is not issued, Plaintiff and the Class will suffer irreparable injury and lack an adequate legal remedy if Level Up experiences a second data breach.

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

188. If an injunction is not issued, the resulting hardship to Plaintiff and Class members far exceeds the minimal hardship that Level Up could experience if an injunction is issued.

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

PRAYER FOR RELIEF

Plaintiff and Class members respectfully request judgment against Level Up and that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing her counsel to represent the Class;

B. Awarding declaratory and other equitable relief as necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Level Up from further unfair and/or deceptive practices;

E. Awarding Plaintiff and the Class damages including applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiff demands a jury trial for all claims so triable.

Date: June 16, 2025

Respectfully submitted,

By: /s/Joshua R. Jacobson
Joshua R. Jacobson
JACOBSON PHILLIPS PLLC
2277 Lee Road, Suite B
Winter Park, FL 32789
T: (321) 447-6461
F: (407) 612-2206
joshua@jacobsonphillips.com

Alex Phillips*
STRAUSS BORRELLI, PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
T: (872) 263-1100
F: (872) 263-1109
raina@straussborrelli.com
**Pro hac vice forthcoming*

Attorneys for Plaintiff and Proposed Class