Filing # 252975170 E-Filed 07/21/2026 07:22:17 PM

IN THE CIRCUIT COURT FOR THE SEVENTEENTH JUDICIAL CIRCUIT IN AND FOR BROWARD COUNTY, FLORIDA

ANTHONY SANTANA, LAURA DELAPAZ, and VINCENT OLMO, individually, and on behalf of all others similarly situated, Plaintiffs, v. **BLANK ROME LLP**, Defendant.	No. Division: **CLASS ACTION COMPLAINT** **DEMAND FOR JURY TRIAL**

Plaintiffs, Anthony Santana, Laura Delapaz, and Vincent Olmo ("Plaintiffs"), by and through undersigned counsel, individually and on behalf of all others similarly situated, bring this Class Action Complaint against Defendant, Blank Rome LLP ("Defendant"), alleging as follows.

NATURE OF ACTION

1. This class action arises from Defendant's failure to properly secure and safeguard Plaintiff's and Class Members' sensitive protected health information ("PHI") and personally identifiable information ("PII") from a foreseeable, preventable data breach, which, as a result, has been disclosed to cybercriminals and posted on the dark web.

2. This class action arises from Defendant's failure to protect highly sensitive data.

3. Defendant is a nationwide law firm that offers a wide variety of legal services to its clients. As such, Defendant stores a litany of highly sensitive PII and PHI about its current and former clients—Plaintiffs and Class Members—including their addresses, email addresses, phone numbers, dates of birth, taxpayer identification numbers, driver's license numbers, state identification card numbers, passport numbers, other government-issued identification numbers,

financial account numbers, payment card information, medical information, and health insurance information (collectively, "Private Information").

4. Due to Defendant's failure to protect the client data it collected through reasonable or adequate security measures, an unauthorized third-party accessed Defendant's network systems and targeted, accessed, and exfiltrated Plaintiff's and Class Members' insufficiently safeguarded Private Information from Defendant's care, causing widespread injuries to Plaintiff and the Class (the "Data Breach").

5. Criminal hackers were able to breach Defendant's systems and steal Plaintiffs' and Class Members' Private Information stored therein because Defendant failed to maintain reasonable security safeguards or protocols to protect that highly sensitive data. In short, Defendant's data security failures placed the Class's Private Information in a vulnerable position, rendering it an easy target for cybercriminals.

6. The exposure of one's Private Information to cybercriminals is a bell that cannot be unrung. Before this Data Breach, Defendant's current and former clients' Private Information was exactly that—private. But now, due to Defendant's wrongful acts and omissions as detailed herein, Plaintiff's and Class Members' Private Information is forever exposed and unsecure.

7. Hackers targeted and obtained Plaintiff's and Class Members' Private Information from Defendant's systems because of the data's value in exploiting and stealing their identities. As a direct and proximate result of Defendant's inadequate data security and breaches of its duties to handle Private Information with reasonable care, the risk of identity theft caused by this Data Breach is impending and has materialized, as Plaintiffs' and Class Members' Private Information was targeted, accessed, and misused, including through its dissemination on the dark web. This present and continuing risk to victims of the Data Breach will remain for their respective lifetimes.

8. As a result of the Data Breach, Plaintiff and Class Members, suffered concrete injuries in fact including, but not limited to (a) costs mitigating the materialized and imminent risk of identity theft; (b) loss of time and productivity mitigating the materialized and imminent risk of identity theft; (c) actual identity theft and fraud; (d) costs and lost time due to actual identity theft; (e) deprivation of value of their Private Information; (f) loss of privacy; (g) emotional distress; and (h) the continued risk to their Private Information, which remains subject to further breaches so long as Defendant fails to undertake adequate measures to protect it.

PARTIES

9. Plaintiff Anthony Santana is a natural person and citizen of Vallejo, California, where he intends to remain.

10. Plaintiff Laura Delapaz is a natural person and citizen of Encino, California, where she intends to remain.

11. Plaintiff Vincent Olmo is a natural person and citizen of San Diego, California, where he intends to remain.

12. Defendant is a limited liability general partnership formed under the laws of Pennsylvania and with its principal place of business at One Logan Square, 130 North 18th Street, Philadelphia, PA 19103. Defendant has multiple locations in the state of Florida, including in West Palm Beach, Florida.

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action pursuant to Fla. Stat. §§ 26.012 and 86.011, because this Complaint seeks damages in excess of $50,000.00 dollars, exclusive of interest and attorneys' fees.

14. This Court has personal jurisdiction over Defendant under Fla. Stat. § 48.193(2) because Defendant is a Florida citizen and because Defendant is engaged in substantial and not isolated activity within this state.

15. Venue is proper in this forum pursuant to Fla. Stat. § 47.011 because Defendant failed to safeguard Plaintiffs' and Class Members' Private Information in this County and the causes of action accrued in this County.

BACKGROUND

A. Defendant Collected and Stored Plaintiffs' and Class Members' Private Information

16. Defendant is a nationwide law firm that offers a wide variety of legal services. As part of its business, Defendant receives and maintains the Private Information of thousands of its current and former clients, including Plaintiffs and Class Members.

17. Plaintiff and Class Members entrusted their Private Information to Defendant as a required condition and in exchange for receiving services from Defendant.

18. At all relevant times, Defendant knew it was using its systems to manage, store, and transmit valuable, sensitive Private Information, and that as a result, those systems would be attractive targets for cybercriminals.

19. Defendant also knew that any breach of its information technology systems and exposure of the data stored therein would result in the increased risk of identity theft and fraud for the thousands of individuals whose Private Information is compromised, as well as intrusion into those individuals' sensitive health matters.

20. Defendant derived economic benefits from collecting Plaintiff's and Class Members' Private Information. Without the required submission of Private Information, Defendant could not perform its operations or generate revenue, including by billing for services

provided.

21. As a result of collecting and storing the Private Information of Plaintiff and Class Members for its own financial benefit, Defendant had a continuous duty to adopt and employ reasonable measures to protect Plaintiff's and the Class Members' Private Information from wrongful disclosure.

22. In exchange for receiving Plaintiff's and Class Members' Private Information, Defendant promised to safeguard the sensitive and confidential data, to use it only for authorized purposes, and to delete it from its systems once there was no longer a need to maintain it.

23. In its mandatory collection and use of Plaintiffs' and Class Members' Private Information, Defendant also agreed it would safeguard the data in accordance with its internal policies, state law, and federal law. After all, Plaintiffs and Class Members themselves took reasonable steps to secure their Private Information against wrongful disclosure and misuse.

24. But for Defendant's promises to keep their Private Information secure and confidential, Plaintiffs and Class Members would not have sought services from or entrusted their Private Information to Defendant.

25. Thus, Plaintiffs and Class Members provided their Private Information to Defendant with the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access.

B. Defendant's Data Security Failures Caused the Data Breach.

26. On or around May 21, 2026, unauthorized cybercriminals posed as Blank Rome IT employees and gained access to Defendant's inadequately protected computer system and

Plaintiffs' and the Class Member's Private Information stored thereon. Upon information and belief, the Defendant has not publicly disclosed the threat actor involved in the Breach.[1]

27. The Defendant investigated the Data Breach and disclosed in its Notice Letter that at least the following sensitive personal information was involved in the Data Breach: addresses, email addresses, phone numbers, dates of birth, taxpayer identification numbers, driver's license numbers, state identification card numbers, passport numbers, other government-issued identification numbers, financial account numbers, payment card information, medical information, and health insurance information.[2]

28. While the Breach occurred on or about May 21, 2026, Blank Rome delayed noticing affected individuals until around June 26, 2026, when Blank Rome began mailing notice letters ("Notice Letter") to affected individuals. Defendant's delay in alerting impacted individuals of the Breach prevented Plaintiffs and Class Members from taking earlier actions to protect themselves against fraud and misuse of their information.[3]

29. Defendant's delayed notice of the Breach leaves impacted individuals with no information regarding critical facts about the Data Breach, such as details of the root cause of the Breach, the vulnerabilities exploited, when the Breach occurred, and the remedial measures taken by Defendant, if any.

30. Defendant failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access and exploitation.

[1] https://oag.ca.gov/system/files/Blank%20Rome%20-%20California%20Notification.pdf (last visited July 21, 2026).
[2] *Id.*
[3] *Id.*

31. Defendant failed to timely notify Plaintiffs and Class Members of the Data Breach, preventing Plaintiffs and Class Members from taking earlier action to protect their Private Information.

32. By collecting, storing, and maintaining the Private Information of Plaintiffs and Class Members, Defendant owed a duty to Plaintiffs and Class Members to protect and safeguard their Private Information from unauthorized disclosures.

33. Plaintiffs' and Class Members' Private Information was targeted, accessed, and stolen by cybercriminals in the Data Breach. Defendant's deficient security for Private Information caused and allowed criminals to target and take files containing Plaintiffs' and Class Members' inadequately protected, unencrypted Private Information in Defendant's possession through the Data Breach.

34. Because Defendant had a duty to protect Plaintiffs' and Class Members' Private Information, Defendant should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information. Thus, Defendant had a duty to ensure that Class Members' Private Information, stored within its networks and systems, was secured and protected from unauthorized disclosures to third parties.

35. Defendant could and should have prevented this Data Breach by ensuring the files and servers containing Plaintiffs' and Class Members' Private Information were properly secured and encrypted but failed to do so.

36. Plaintiffs further believe that their Private Information and that of Class Members, was subsequently sold on the dark web following the Data Breach, as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

37. All in all, Defendant failed to take the necessary precautions required to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized access and exploitation.

38. Defendant's actions represent a flagrant disregard of the rights of Plaintiffs and the Class, both as to privacy and property.

39. As such, Plaintiffs and the Class have suffered harm and continue to be at an imminent and impending risk of identity theft and fraud.

C. Defendant Knew the Risk of this Data Breach.

40. Defendant's negligence in failing to safeguard Plaintiffs' and Class Members' Private Information is exacerbated by the repeated warnings and alerts regarding the need to protect and secure sensitive data.

41. Data thieves regularly target businesses like Defendant due to the highly sensitive information such entities maintain. Defendant knew and understood that unprotected Private Information is highly sought after by criminals who seek to illegally monetize that Private Information through unauthorized access.

42. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in recent years. In light of past high profile data breaches at industry-leading companies, including, for example, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Defendant knew or, if acting as a reasonable business, should have known that the Private Information it collected and maintained would be vulnerable to and targeted by cybercriminals.

43. In 2024, a 3,158 data breaches occurred, exposing approximately 1,350,835,988 sensitive records—a 211% increase year-over-year.

44. Indeed, cyberattacks have become so notorious that the Federal Bureau of Investigation 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."[4]

45. Entities in custody of PHI, like Defendant, reported the largest number of data breaches among all measured sectors in 2022, with the highest rate of exposure per breach. Indeed, when compromised, health related data is among the most sensitive and personally consequential. A report focusing on health breaches found the "average total cost to resolve an identity theft-related incident . . . came to about $20,000," and victims were often forced to pay out of pocket costs for healthcare they did not receive in order to restore coverage.[5] Almost 50% of the victims lost their healthcare coverage as a result, while nearly 30 percent said their insurance premiums went up.

46. PHI is particularly valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can be used to create fake insurance claims, allowing for the purchase and resale of medical equipment, or gain access to prescriptions for illegal use or resale.

---

[4] 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 (last visited July 21, 2026).

[5] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET, March 3, 2010, available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited July 21, 2026).

47. As indicated by Jim Trainor, second in command at the FBI's cyber security division: "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place. Credit cards can be, say, five dollars or more where PHI records can go from $20 say up to—we've even seen $60 or $70."[6] A complete identity theft kit with health insurance credentials may be worth up to $1,000 on the black market, whereas stolen payment card information sells for about $1.

48. As a business in possession of Private Information, Defendant knew, or should have known, the importance of safeguarding the Private Information entrusted to it and of the foreseeable consequences if its systems were breached, including the significant costs that would imposed on Plaintiff and Class Members. Nevertheless, Defendant failed to implement or follow reasonable cybersecurity measures.

49. Given the nature of the Data Breach, it was foreseeable that Plaintiff's and Class Members' Private Information compromised therein would be targeted by hackers and cybercriminals for use in variety of different injurious ways. Indeed, the cybercriminals who possess Plaintiff's and Class Members' Private Information can easily obtain their tax returns or open fraudulent credit card accounts in Plaintiff's and Class Members' names.

50. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on its systems, amounting to tens of thousands of individuals' detailed Private Information, and, thus, that these individuals would be harmed by the unauthorized disclosure of that unencrypted data.

[6] You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows, IDExperts, May 14, 2015, https://www.idexpertscorp.com/knowledge-center/single/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat (last visited July 21, 2026).

51. Plaintiff and Class Members were the foreseeable and probable victims of Defendant's inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing Private Information and the critical importance of providing adequate security for that information.

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

D. Defendant Was Required, But Failed, to Follow FTC Rules.

53. 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.

54. 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. The FTC declared that, *inter alia*, businesses must do the following:

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.

55. 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.

56. Furthermore, the FTC explains that companies must do the following:

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.

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

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

E. Defendant Violated HIPAA.

59. HIPAA circumscribes security provisions and data privacy responsibilities designed to keep clients' 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.

60. HIPAA provides specific privacy rules that require comprehensive administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of Private Information and PHI is properly maintained. *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).

61. The Data Breach itself resulted from a combination of inadequacies showing As a covered entity, Defendant failed to comply with safeguards mandated by HIPAA. Defendant's security failures include, but are not limited to the following:

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);

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 Defendant'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).

F. Defendant Failed to Follow Industry Standards.

62. 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); MFA; backup data; and limiting which employees can access sensitive data.

63. Other industry standard best practices Defendant should have followed 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.

64. Additionally, to mitigate cyber threats from ransomware gangs specifically, the Joint Cybersecurity and Infrastructure Security Agency ("CISA") recommends rudimentary actions that businesses like Defendant should take: (a) installing updates for operating systems, software, and firmware as soon as they are released; (b) requiring phishing-resistant MFA (i.e., non-SMS text based) for as many services as possible; and (c) training users to recognize and report phishing attempts. Defendant failed to implement the foregoing CISA-recommended measures, which failures caused and allowed the Data Breach.

65. Defendant 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) and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness. These frameworks are applicable and accepted industry standards.

66. By failing to comply with these accepted industry standards, Defendant opened the door for cybercriminals to target, access, and steal Plaintiff's and Class Members' Private Information in the Data Breach.

G. Defendant Owed Common Law Duties to Safeguard Private Information.

67. In addition to its obligations under federal and state laws, Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the Private Information in its possession from being compromised, lost, stolen, accessed, and misused by unauthorized persons. These duties obligated Defendant to provide reasonable data security consistent with industry standards to protect

Plaintiffs' and Class Members' Private Information in its care from unauthorized disclosure.

68. Defendant owed a duty to Plaintiff sand Class Members to create and implement reasonable data security practices and procedures to protect their Private Information, including adequately training its employees and others who accessed Private Information on how to adequately protect it.

69. Defendant owed a duty to Plaintiffs and Class Members to implement processes that would detect a compromise of Private Information in a timely manner.

70. Defendant owed a duty to Plaintiffs and Class Members to act upon data security warnings and alerts in a timely fashion.

71. Defendant owed a duty to Plaintiffs and Class Members to disclose in a timely and accurate manner when and how the Data Breach occurred.

72. Defendant owed a duty to Plaintiffs and Class Members because they were foreseeable and probable victims of any inadequate data security practices.

73. Defendant failed to take the necessary precautions to safeguard and protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure. Defendant's actions and omissions in breach of its duties of care represent a flagrant disregard of Plaintiffs' and Class Members' rights.

H. Plaintiffs and Class Members Suffered Common Injuries and Damages.

74. Because of Defendant's failure to prevent the Data Breach through reasonable, standard, or legally compliant measures, Plaintiff and Class Members suffered, and will continue to suffer, a host of injuries and damages. These injuries include, *inter alia*, monetary losses, lost time, anxiety, and emotional distress, as well as the following harms Plaintiffs and Class Members have suffered and will continue to experience, without limitation:

a. actual identity theft, fraud, and misuse;

b. the imminent, increased risk of identity theft, fraud, and misuse;

c. loss of the opportunity to control how their Private Information is used;

d. diminution in value of their Private Information;

e. compromise and continuing publication of their Private Information;

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

g. 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; and

h. continued risk to their Private Information, which remains in Defendant's possession at risk for future breach, so long as Defendant fails to take appropriate measures to protect it.

75. Plaintiffs further believe their Private Information, and that of Class Members, will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type and that visit dark web pages like the Inc Ransom leak site.

76. The risk of identity theft is not speculative or hypothetical; it is impending and materialized, as Plaintiff's Private Information was targeted and accessed by cybercriminals, and has already been misused by dissemination on the dark web.

Imminent Risk of Identity Theft and Fraud

77. Plaintiffs and Class Members are at a heightened risk of identity theft for years to come because of the Data Breach.

78. The link between a data breach and the risk of identity theft is simple and well established. Criminals acquire and steal Private Information to monetize it. Criminals monetize the data by selling the stolen information on the internet black market to other criminals who then utilize the information to commit a variety of identity theft related crimes discussed below.

79. Stolen Private Information is one of the most valuable commodities of information on the black market. According to Experian, a credit-monitoring service, stolen Private Information can be worth up to $1,000.00 depending on the type of information obtained.

80. The value of Plaintiffs' and the Class's Private Information on the black market is considerable. Stolen Private Information trades on the black market for years. And criminals frequently post and sell stolen information openly and directly on the dark web, further exposing the data.

81. It can take victims years to discover such identity theft and fraud. This gives criminals plenty of time to sell the Private Information far and wide.

82. One way that criminal's profit from stolen Private Information is by creating comprehensive dossiers on individuals called "Fullz" packages. These dossiers are both shockingly accurate and comprehensive. Criminals create them by cross-referencing and combining two sources of data—first the stolen Private Information, and second, unregulated data found elsewhere on the internet (like phone numbers, emails, addresses, etc.).

83. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the Private Information stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

84. The development of Fullz packages means that the Private Information exposed in the Data Breach can easily be linked to data of Plaintiffs and the Class that is available on the internet or other sources. That is exactly what is happening to Plaintiffs and Class Members, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other Class Members' stolen Private Information is being misused, and that such misuse is fairly traceable to the Data Breach.

85. Defendant disclosed Plaintiffs' and Class Members' Private Information for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed their Private Information to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen Private Information.

86. Theft of PHI, in particular, is gravely serious as well: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[7]

87. PHI is also used in detrimental ways, including by leveraging sensitive personal health details and diagnoses to extort or coerce someone, and serious and long-term identity theft.

88. Victims of identity theft also often suffer embarrassment, blackmail, or harassment in person or online, and/or experience financial losses resulting from fraudulently opened accounts or misuse of existing accounts.

[7] *See* Federal Trade Commission, Medical Identity Theft, http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited July 21, 2026).

89. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen Private Information. To protect themselves, Plaintiff and Class Members will need to remain vigilant for years or even decades to come.

Costs and Lost Time Mitigating the Risk of Identity Theft and Fraud

90. To date, Defendant has done little to provide Plaintiffs and Class Members with relief for the damages they suffered due to the Data Breach.

91. As a result of the recognized risk of identity theft, when a data breach occurs, and an individual is notified that their Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm—yet the asset of time has been lost.

92. In the event that Plaintiffs and Class Members experience actual identity theft and fraud, the United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face substantial costs and time to repair the damage to their good name and credit record.

93. Thus, due to the actual and imminent risk of identity theft, Plaintiffs and Class Members must monitor their financial accounts for many years to mitigate that harm.

94. Plaintiffs and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover.

95. These efforts are consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[8]

96. Given the type of targeted attack in this case and sophisticated criminal activity, the type of information involved, and the *modus operandi* of cybercriminals, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the dark web for sale and purchase by criminals intending to utilize the Private Information for identity theft crimes— e.g., opening bank accounts in the victims' names to make purchases or to launder money; filing false tax returns; taking out loans or insurance; or filing false unemployment claims.

97. Once Private Information is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse.

98. Such fraud may go undetected until collection calls commence months or even years later. An individual may not know that their information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an authentic tax return is rejected.

99. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel their cards and request a replacement. The information

[8] *See Federal Trade Commission*, IDENTITYTHEFT.GOV, https://www.identitytheft.gov/Steps (last visited July 21, 2026).

disclosed in this Data Breach (Social Security numbers and medical histories, for example) is impossible to "close" and difficult, if not impossible, to change.

100. Consequently, Plaintiffs and Class Members are at a present and ongoing risk of fraud and identity theft for many years into the future, making the present and future cost of credit and identity theft monitoring reasonable and necessary.

101. For this reason, Plaintiffs and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, as a result of Defendant's conduct that caused the Data Breach.

102. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more a year per Class Member. This is a reasonable and necessary cost to protect Class Members from the risk of identity theft that arose from Defendant's Data Breach. This is a future cost for a minimum of five years that Plaintiffs and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

Diminished Value of Private Information

103. Personal data like Private Information is a valuable property right. Its value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

104. An active and robust legitimate marketplace for personal information also exists. In 2019, the data brokering industry was worth roughly $200 billion.

105. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $60 a year.

106. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which have an inherent market value in both legitimate and black markets, has been damaged and diminished in its value by its unauthorized and likely release onto the dark web, where holds significant value for the threat actors.

107. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the data has been lost, thereby causing additional loss of value.

Lost Benefit of the Bargain

108. Furthermore, Defendant's poor data security deprived Plaintiffs and Class Members of the benefit of their bargain.

109. When agreeing to provide their Private Information, which was a condition precedent to obtain medical services from Defendant, Plaintiffs and Class Members, as clients, understood and expected that they were, in part, paying for services and data security to protect the Private Information they were required to provide.

110. Plaintiffs value data security. Indeed, data security is an important consideration of seeking legal services.

111. In 2024, the technology and communications conglomerate Cisco published the results of its multi-year Consumer Privacy Survey. Therein, Cisco reported the following:

> For the past six years, Cisco has been tracking consumer trends across the privacy landscape. During this period, privacy has evolved from relative obscurity to a customer requirement with more than 75% of consumer respondents saying they won't purchase from an organization they don't trust with their data. [9]

[9] *Privacy Awareness: Consumers Taking Charge to Protect Personal*, CISCO, https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-report-2024.pdf (last visited July 21, 2026).

112. The same survey found, "Privacy has become a critical element and enabler of customer trust, with 94% of organizations saying their customers would not buy from them if they did not protect data properly." And 89% of consumers stated, "I care about data privacy," while 83% of consumers declared, "I am willing to spend time and money to protect data," and, "I expect to pay more" for privacy.

113. Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class Members received services of a lesser value than what they reasonably expected to receive under the bargains struck with Defendant.

I. Plaintiffs' Experiences and Injuries

Plaintiff Anthony Santana

114. At all times relevant, Plaintiff Santana was a client of Defendant. As a condition of receiving services, Plaintiff Santana provided Defendant with his Private Information.

115. At the time of the Data Breach, Defendant maintained Plaintiff Santana's Private Information in Defendant's systems with inadequate data security, causing cybercriminals to target, access, and steal Plaintiff Santana's Private Information in the Data Breach.

116. Plaintiff Santana is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe manner. He is careful to store any documents containing his Private Information in a secure location.

117. Plaintiff Santana provided his Private Information to Defendant relying on Defendant to use reasonable measures to protect it, according to Defendant's internal policies as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Santana's

Private Information on its systems and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

118. Plaintiff Santana reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of Private Information.

119. On information and belief, Plaintiff Santana's Private Information has already been published by cybercriminals on the dark web.

120. Plaintiff Santana further believes his Private Information, and that of Class Members, will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

121. The risk of identity theft is not speculative or hypothetical; it is impending and materialized, as there is evidence Plaintiff Santana's Private Information was targeted, accessed by cybercriminals, and misused by dissemination on the dark web.

122. Plaintiff Santana has spent, and will continue to spend, significant time and effort monitoring his accounts to protect himself from identity theft as a result of the Data Breach, which lost time is an additional injury Defendant's data security failures caused. Because of the Data Breach, Plaintiff Santana anticipates spending considerable amounts of time and money to try and mitigate his injuries.

123. Additionally, as a result of and since the Data Breach, Plaintiff Santana has suffered from a spike in spam and scam text messages, phone calls and emails.

124. Plaintiff Santana fears for his personal financial security and worries about what information was exposed in the Data Breach, and about cybercriminals further misusing his Private Information. Because of Defendant's Data Breach, Plaintiff Santana has suffered, and will continue to suffer, from anxiety, depression, and fear of identity theft. Such injuries go far beyond

allegations of mere worry or inconvenience. Rather, Plaintiff Santana's injuries are precisely the type of injuries that the law contemplates and addresses.

125. Plaintiff Santana also suffered actual injury from the exposure and theft of his Private Information, which violates his rights to privacy.

126. Plaintiff Santana suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property, which Defendant was required but failed to adequately protect.

127. Plaintiff Santana suffered imminent and impending injury arising from the actual misuse of his Private Information and attendant substantially increased risk of fraud, misuse, and identity theft, all because Defendant's Data Breach placed Plaintiff Santana's Private Information right in the hands of criminals.

128. Today, Plaintiff Santana has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

Plaintiff Laura Delapaz

129. At all times relevant, Plaintiff Delapaz was a client of Defendant. As a condition of receiving services, Plaintiff Delapaz provided Defendant with her Private Information.

130. At the time of the Data Breach, Defendant maintained Plaintiff Delapaz's Private Information in Defendant's systems with inadequate data security, causing cybercriminals to target, access, and steal Plaintiff Delapaz's Private Information in the Data Breach.

131. Plaintiff Delapaz is very careful about her Private Information's privacy and security. She does not knowingly transmit her Private Information over the internet in an unsafe manner. She is careful to store any documents containing her Private Information in a secure location.

132. Plaintiff Delapaz provided her Private Information to Defendant relying on Defendant to use reasonable measures to protect it, according to Defendant's internal policies as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Delapaz's Private Information on its systems and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

133. Plaintiff Delapaz reasonably understood that a portion of the funds she paid to Defendant would be used to pay for adequate cybersecurity and protection of Private Information.

134. Plaintiff Delapaz has spent, and will continue to spend, significant time and effort monitoring her accounts to protect herself from identity theft as a result of the Data Breach, which lost time is an additional injury Defendant's data security failures caused. Because of the Data Breach, Plaintiff Delapaz anticipates spending considerable amounts of time and money to try and mitigate her injuries.

135. Additionally, as a result of and since the Data Breach, Plaintiff Delapaz has suffered from a spike in spam and scam text messages, phone calls and emails using her compromised Private Information, evidencing that her Private Information is being misused.

136. Plaintiff Delapaz fears for her personal financial security and worries about cybercriminals further misusing her Private Information stolen in the Data Breach to commit identity theft and further crimes against Plaintiff. Because of Defendant's Data Breach, Plaintiff Delapaz has suffered, and will continue to suffer from anxiety, depression, and fear of identity theft. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Delapaz's injuries are precisely the type of injuries that the law contemplates and addresses.

137. Plaintiff Delapaz also suffered actual injury from the exposure and theft of her Private Information, which violates her rights to privacy.

138. Plaintiff Delapaz suffered actual injury in the form of damages to and diminution in the value of her Private Information. After all, Private Information is a form of intangible property, which Defendant was required to adequately protect.

139. Plaintiff Delapaz suffered imminent and impending injury arising from actual misuse of her Private Information and the substantially increased risk of fraud, misuse, and identity theft, all because Defendant's deficient data security and the consequential Data Breach that placed Plaintiff Delapaz's Private Information right in the criminal hackers' hands.

140. Plaintiff Delapaz further believes her Private Information, and that of Class Members, will be sold and further disseminated on the dark web following the Data Breach as that is the modus operandi of cybercriminals that commit cyber-attacks of this type.

141. The risk of identity theft is not speculative or hypothetical; it is impending and materialized, as Plaintiff Delapaz's Private Information was targeted and accessed by cybercriminals, and has already been misused by dissemination on the dark web.

142. Today, Plaintiff Delapaz has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from additional breaches.

Plaintiff Vincent Olmo

143. At all times relevant, Plaintiff Olmo was a client of Defendant. As a condition of receiving services, Plaintiff Olmo provided Defendant with his Private Information.

144. At the time of the Data Breach, Defendant maintained Plaintiff Olmo's Private Information in Defendant's systems with inadequate data security, causing cybercriminals to target, access, and steal Plaintiff Olmo's Private Information in the Data Breach.

145. Plaintiff Olmo is very careful about the privacy and security of his Private Information. He does not knowingly transmit his Private Information over the internet in an unsafe

manner. He is careful to store any documents containing his Private Information in a secure location.

146. Plaintiff Olmo provided his Private Information to Defendant relying on Defendant to use reasonable measures to protect it, according to Defendant's internal policies as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Olmo's Private Information on its systems and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

147. Plaintiff Olmo reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of Private Information.

148. On information and belief, Plaintiff Olmo's Private Information has already been published by cybercriminals on the dark web.

149. Plaintiff Olmo further believes his Private Information, and that of Class Members, will be sold and further disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

150. The risk of identity theft is not speculative or hypothetical; it is impending and materialized, as there is evidence Plaintiff Olmo's Private Information was targeted, accessed by cybercriminals, and misused by dissemination on the dark web.

151. Plaintiff Olmo has spent, and will continue to spend, significant time and effort monitoring his accounts to protect himself from identity theft as a result of the Data Breach, which lost time is an additional injury Defendant's data security failures caused. Because of the Data Breach, Plaintiff Olmo anticipates spending considerable amounts of time and money to try and mitigate his injuries.

152. Additionally, as a result of and since the Data Breach, Plaintiff Olmo has suffered from a spike in spam and scam text messages, phone calls and emails.

153. Plaintiff Olmo fears for his personal financial security and worries about what information was exposed in the Data Breach, and about cybercriminals further misusing his Private Information. Because of Defendant's Data Breach, Plaintiff Olmo has suffered, and will continue to suffer, from anxiety, depression, and fear of identity theft. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Olmo's injuries are precisely the type of injuries that the law contemplates and addresses.

154. Plaintiff Olmo also suffered actual injury from the exposure and theft of his Private Information, which violates his rights to privacy.

155. Plaintiff Olmo suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property, which Defendant was required but failed to adequately protect.

156. Plaintiff Olmo suffered imminent and impending injury arising from the actual misuse of his Private Information and attendant substantially increased risk of fraud, misuse, and identity theft, all because Defendant's Data Breach placed Plaintiff Olmo's Private Information right in the hands of criminals.

157. Today, Plaintiff Olmo has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from additional breaches.

CLASS ACTION ALLEGATIONS

158. Plaintiffs bring this class action, under Rule 1.220(b)(2), (b)(3), and (d)(4) of the Florida Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All individuals residing in the United States whose Private Information was compromised in the Data Breach.

159. Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, officer or director of those entities, any successor or assign, and the Judge(s) overseeing the action, including their staff and immediate family.

160. Plaintiffs reserve the right to amend the class definition.

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

162. Ascertainability. All members of the proposed Class are readily ascertainable from information in Defendant's custody and control.

163. Numerosity. The Class Members are so numerous that joinder of all Class Members is impracticable.

164. Typicality. Plaintiffs' 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.

165. Adequacy. Plaintiffs will fairly and adequately protect the proposed Class's common interests. Their interests do not conflict with Class Members' interests. And Plaintiffs have 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.

166. Commonality and Predominance. Plaintiffs' 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. whether Defendant had a duty to use reasonable care in safeguarding Plaintiffs' and the Class's Private Information;

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

c. whether Defendant were negligent in maintaining, protecting, and securing Private Information;

d. whether Defendant breached contract promises to safeguard Plaintiffs' and the Class's Private Information;

e. whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

f. whether the Data Breach caused Plaintiffs and the Class injuries;

g. what the proper damages measure is; and

h. whether Plaintiffs and the Class are entitled to damages, treble damages, and or injunctive relief.

167. Superiority. A class action will provide substantial benefits and is superior to all other available means for the fair and efficient adjudication of this controversy. The damages or other financial detriment suffered by individual Class Members are relatively small compared to the burden and expense that individual litigation against Defendant would require. Thus, it would be practically impossible for Class Members, on an individual basis, to obtain effective redress for their injuries. Not only would individualized litigation increase the delay and expense to all parties

and the courts, but individualized litigation would also create the danger of inconsistent or contradictory judgments arising from the same set of facts. By contrast, the class action device provides the benefits of adjudication of these issues in a single proceeding, ensures economies of scale, provides comprehensive supervision by a single court, and presents no unusual management difficulties.

CAUSES OF ACTION

COUNT I: NEGLIGENCE/NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Class)

168. Plaintiffs restate and reallege the allegations in the preceding paragraphs 1–167 as if fully set forth herein.

169. Plaintiff and Class Members entrusted their Private Information to Defendant as a condition of receiving Defendant's services.

170. Defendant owed a duty of care to Plaintiff and Class Members to adequately and reasonably safeguard their Private Information because it was foreseeable that Defendant's failure to use adequate data security in accordance with industry standards for data security would compromise their Private Information in a data breach.

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

172. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure to use adequate data security in accordance with industry standards for data security would compromise their Private Information in a data breach.

173. Defendant had full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if their Private Information was wrongfully disclosed.

174. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information 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.

175. The risk that unauthorized persons would attempt to gain access to the Private Information and misuse it was foreseeable. Given that Defendant holds vast amounts of Private Information, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the Private Information, whether by malware or otherwise.

176. Private Information is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the Private Information of Plaintiffs and Class Members and the importance of exercising reasonable care in handling it.

177. Defendant 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 Private Information, 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.

178. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

179. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required

and necessary for Plaintiffs and Class Members to take appropriate measures to protect their Private Information, 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.

180. As such, Defendant owed Plaintiff and Class Members the following duties of care, among others:

a. To exercise reasonable care in handling and using the Private Information in its care and custody;

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

c. To promptly detect attempts at unauthorized access;

d. To notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their Private Information.

181. Defendant owed these duties to Plaintiffs and Class Members because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security practices. After all, Defendant actively sought and obtained Plaintiffs' and Class Members' Private Information.

182. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

183. Defendant also had a duty to exercise appropriate clearinghouse practices to remove Private Information it was no longer required to retain under applicable regulations.

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

185. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class entrusted Defendant with their confidential Private Information, a necessary part of obtaining services from Defendant.

186. Under the FTCA, 15 U.S.C. § 45, Defendant had a duty to use fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class Members' Private Information.

187. Section 5 of the FTCA 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 Private Information entrusted to it. The FTC publications and orders promulgated pursuant to the FTCA also form part of the basis of Defendant's duty to protect Plaintiffs' and the Class Members' sensitive Private Information.

188. Defendant violated its duty under section 5 of the FTCA by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information Defendant 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.

189. Similarly, under HIPAA, Defendant had a duty to follow HIPAA standards for privacy and security practices to protect Plaintiffs' and Class Members' Private Information.

190. Defendant violated its duty under HIPAA by failing to use reasonable measures to protect its Private Information and by not complying with applicable regulations detailed *supra*. Here too, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information that Defendant 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.

191. Plaintiffs and Class Members are within the class of persons the FTCA and HIPAA were enacted to protect.

192. The harm Plaintiffs and Class Members suffered due to Defendant's conduct in violation of the FTCA and HIPAA is the type of harm these statutes and regulations were enacted to prevent.

193. Defendant's violations of the FTCA and HIPAA constitute negligence *per se*.

194. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

195. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' Private Information by disclosing and providing access to this information to unauthorized third parties and by failing to ensure the Private Information was stored, used, and exchanged, in a manner that kept it sufficiently protected.

196. Defendant 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 Private Information of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs and Class Members' injury.

197. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class Members' injuries-in-fact.

198. As a direct and proximate result of Defendant's negligence Plaintiffs and Class Members have suffered or will suffer damages and injuries as set forth herein, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

199. Plaintiffs and Class Members are entitled to damages, including in an amount to be proven at trial.

COUNT II: BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

200. Plaintiffs restate and reallege the allegations in the preceding paragraphs 1–167 as if fully set forth herein.

201. Defendant required Plaintiffs and Class Members to provide and entrust their Private Information to Defendant as a condition of obtaining services.

202. When Plaintiffs and Class Members provided their Private Information and/or payment to Defendant, they formed implied contracts pursuant to which Defendant agreed to safeguard and protect such Private Information and to timely and accurately notify Plaintiffs and Class Members if and when their Private Information was breached and compromised.

203. The valid and enforceable implied contracts Plaintiffs and Class Members formed with Defendant included Defendant's implied promises to protect Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

204. Defendant's mandatory collection of Plaintiffs' and Class Members' Private Information gave rise to Defendant's implied promise and contractual duty to maintain the privacy and confidentiality of that Private Information and to keep it safeguarded against unauthorized access and disclosure.

205. Defendant's adequate protection of Plaintiffs' and Class Members' Private Information was a material aspect of these implied contracts with Defendant.

206. In entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with industry standards and relevant laws and regulations, including the FTCA and HIPAA.

207. Plaintiffs and Class Members who provided their Private Information to Defendant reasonably believed and expected that Defendant would adequately employ adequate data security to protect that Private Information. Defendant failed to do so.

208. A meeting of the minds occurred when Defendant required Plaintiffs and the Class Members to provide their Private Information as a mandatory condition to their receipt of legal services and when Plaintiffs and Class Members agreed to, and did, provide their Private Information to Defendant.

209. Defendant materially breached its contractual obligations to protect the Private Information it required Plaintiffs and Class Members to provide when that Private Information was unauthorizedly disclosed in the Data Breach due to Defendant's inadequate data security measures and procedures.

210. Defendant materially breached its contractual obligations to deal in good faith with Plaintiffs and Class Members when it failed to take adequate precautions to prevent the Data Breach and failed to promptly notify Plaintiffs and Class Members of the Data Breach.

211. Defendant materially breached the terms of its implied contracts, including but not limited to by failing to comply with industry standards or the standards of conduct embodied in statutes like Section 5 of the FTCA, by failing to otherwise protect Plaintiffs' and Class Members' Private Information, as set forth *supra*.

212. The Data Breach was a reasonably foreseeable consequence of Defendant's conduct in breach of these implied contracts with Plaintiffs and Class Members.

213. As a direct and proximate result of Defendant's breach of their implied contracts with Plaintiff and Class Members and the attendant Data Breach, Plaintiffs and Class Members have suffered injuries and damages as set forth herein and have been irreparably harmed, as well as suffering and the loss of the benefit of the bargain they struck with Defendant.

214. Plaintiff and Class Members are entitled to damages, including compensatory, and/or nominal damages, and/or restitution, in an amount to be proven at trial.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

215. Plaintiffs restate and reallege the allegations in the preceding paragraphs 1–167 as if fully set forth herein.

216. Plaintiffs and Class Members conferred benefits upon Defendant: Defendant benefitted by using Plaintiffs' and Class Members' Private Information to provide and receive payment for Defendant's services, and by accepting payment from or on behalf of Plaintiffs and Class Members.

217. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members.

218. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the Private Information that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

219. The money Plaintiffs and Class Members paid to Defendant included a premium for Defendant's cybersecurity obligations and was supposed to be used by Defendant, in part, to pay for the administrative and other costs of providing reasonable data security and protection for Plaintiffs' and Class Members' Private Information.

220. Additionally, an adequate portion of the money Defendant gained through using Plaintiffs' and Class Members' Private Information should have been reinvested towards the administrative and other costs of providing reasonable data security and protection for Plaintiffs' and Class Members' Private Information.

221. Instead, Defendant enriched itself by saving the costs it reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' Private Information. Rather than providing a reasonable level of security that would have prevented the Data Breach, Defendant instead calculated to increase its own bottom line at Plaintiffs' and Class Members' expense by utilizing cheaper, ineffective security measures and diverting the funds it should have spent on data security to Defendant's own coffers. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

222. Under principles of equity and good conscience, Defendant should not be permitted to retain its ill-gotten gains because Defendant failed to provide adequate safeguards and security measures to protect Plaintiffs' and Class Members' Private Information, which Plaintiffs and Class Members paid for but did not receive.

223. Plaintiffs and Class Members have no adequate remedy at law.

224. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

COUNT IV
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

225. Plaintiffs restate and reallege the allegations in the preceding paragraphs 1-167 as if fully set forth herein.

226. In light of the special relationship between Defendant and its cleints, whereby Defendant became a guardian of Plaintiffs' and Class Members' Private Information (including highly sensitive, confidential, personal, and other PHI). Defendant was a fiduciary, created by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its clients, including Plaintiffs and Class Members. This benefit included (1) the safeguarding of Plaintiffs' and Class Members' Private Information; (2) timely notifying Plaintiffs and Class Members of the Data Breach; and (3) maintaining complete and accurate records of what and where Defendant's clients' Private Information was and is stored.

227. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and the Class upon matters within the scope of its clients' relationship, in particular to keep the Private Information secure.

228. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and the Class by failing to protect their Private Information.

229. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure the confidentiality and integrity of electronic Private

Information Defendant created, received, maintained, and transmitted, in violation of 45 CFR 164.306(a)(1).

230. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to implement technical policies and procedures for electronic information systems that maintain electronic Private Information to allow access only to those persons or software programs that have been granted access rights, in violation of 45 CFR 164.312(a)(1).

231. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to implement policies and procedures to prevent, detect, contain, and correct security violations, in violation of 45 CFR 164.308(a)(1).

232. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii).

233. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic Private Information, in violation of 45 CFR 164.306(a)(2).

234. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to protect against any reasonably-anticipated uses or disclosures of electronic Private Information that are not permitted under the privacy rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3).

235. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to ensure compliance with the HIPAA security standard rules by its workforce, in violation of 45 CFR 164.306(a)(94).

236. Upon information and belief, Defendant breached its fiduciary duties to Plaintiffs and Class Members by impermissibly and improperly using and disclosing Private Information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

237. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer the harms and injuries alleged herein, as well as anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

Plaintiffs and Class Members respectfully request judgment against Defendant and that the Court enter an order as follows:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Class, appointing Plaintiffs as class representatives, and appointing their counsel to represent the Class;

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

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

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

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

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

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

H. Granting other relief that this Court finds appropriate.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial for all claims so triable.

Dated: July 21, 2026

Respectfully submitted,

By: */s/ Jeff Ostrow*
Jeff Ostrow (FBN 121452)
KOPELOWITZ OSTROW P.A.
One W Las Olas Blvd, Suite 500
Ft. Lauderdale, FL 33301
Tel: (954) 525-4100
ostrow@kolawyers.com

Mariya Weekes (FBN 56299)
MILBERG, PLLC
333 SE 2nd Avenue, Suite 2000
Miami, FL 33131
Tel: (866) 252-0878
mweekes@milberg.com

Jason P. Sultzer (*pro hac vice* forthcoming)
SULTZER & LIPARI, PLLC
85 Civic Center Plaza, Suite 200
Poughkeepsie, NY 12601
Tel: (845) 483-7100
sultzerj@thesutlzerlawgroup.com

Attorneys for Plaintiffs and Proposed Class