CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson, Esq. (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart, Esq. (SBN 306499)
yhart@clarksonlawfirm.com
Bryan P. Thompson, Esq. (SBN 354683)
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

COTCHETT, PITRE & McCARTHY, LLP
Thomas E. Loeser, Esq. (SBN: 202724)
tloeser@cpmlegal.com
2716 Ocean Park Blvd., Ste. 3088
Santa Monica, CA 90405
Tel: (206) 802-1272

Counsel for Plaintiffs and the Proposed Class

[Additional counsel on signature page]

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

IN RE: STIIIZY INC., DATA BREACH SECURITY LITIGATION This Document Relates To: *All cases*	Master File No.: 2:25-cv-00490-GW-SSC **CONSOLIDATED CLASS ACTION COMPLAINT** Complaint Filed: January 17, 2025 Trial Date: None Set

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Plaintiffs G.E., Donald Hatch, Bradley Anderson, Daniel Martinez, Lorenzo Montoya, and Elizabeth Orozco-Preza, (collectively "Plaintiffs") individually and on behalf of all others similarly situated, bring this Consolidated Class Action Complaint and allege the following against STIIIZY Inc. ("STIIIZY" or "Defendant"), based upon personal knowledge with respect to themselves and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

INTRODUCTION

1. STIIIZY is a leading US cannabis brand that provides a range of premium cannabis products to retail consumers. Many consumers of STIIIZY's products use them to treat health concerns, such as chronic pain, nausea, and vomiting, including those related to serious diseases such as cancer and multiple sclerosis. STIIIZY frequently markets its products as promoting mental and physical health and well-being.

2. To purchase products from STIIIZY, customers are required to provide STIIIZY with their highly sensitive and personally identifiable information ("PII") and, on some occasions, private health information ("PHI") (collectively "Private Information"), which STIIIZY uses to engage in its usual business activities. Given the stigma associated with cannabis, despite its legal status, even the fact that an individual patronized STIIZY is sensitive information. STIIIZY acknowledges the serious responsibility it bears in safeguarding the data it collects, and makes explicit commitments that it "values your privacy"[1] and "implements security measures designed to protect your information from unauthorized access, disclosure or

[1] *Notice of Data Breach*, STIIIZY (Jan. 7, 2025), https://www.stiiizy.com/pages/notice-of-data-breach?srsltid=AfmBOopaL8d9szOjlv-QGULGYU9lod0KJ02mlxEYilBH5QiaSbKqQmSM ("Notice of Data Breach").

accidental loss or destruction."[2] Despite these assurances to its customers, STIIIZY failed to protect the very Private Information it was entrusted with, compromising the Private Information of hundreds of thousands of its customers, when it allowed unauthorized third parties to access and exfiltrate its customers' Private Information in a data breach, announced by Defendant on January 7, 2025 (the "Data Breach").[3]

3. Specifically, STIIIZY entrusted its point-of-sale vendor with extremely sensitive customer data – including government-issued IDs, medical cannabis cards, transactional histories, and more – without verifying or ensuring that the vendor maintained robust security standards. STIIIZY failed to adequately vet its POS vendor and monitor its security practices and measures, which enabled Everest ransomware group to gain access to Plaintiffs' and Class Members' Private Information. Furthermore, given that Everest has been able to gain access not only to the point-of-sale system itself but also to STIIIZY's own systems, which contained the Private Information, STIIIZY has failed to implement essential and adequate security protocols for its cloud-based software/system. Such failure to enact adequate security protocols – such as enabling access controls and multi-factor authentication, role based permissions, sessions monitoring, encryption of the stored data as well as regular deletion/purging of data no longer necessary, and anomaly detection – left STIIIZY's system vulnerable and open to unauthorized and undetected intrusion.

4. Everest ransomware group is a sophisticated and increasingly prominent threat actor in global cybercrime, known for breaching corporate networks to steal data and installing malicious software that will render servers inoperable unless a ransom is paid.

---

[2] *Privacy Policy*, STIIIZY, https://www.stiiizy.com/policies/privacy-policy.
[3] Notice of Data Breach.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

5. Here, Everest ***already leaked*** the stolen Private Information belonging to Plaintiffs and Class Members on the Dark Web.

6. While STIIIZY has not provided the Data Breach victims, Plaintiffs and Class Members, with a full accounting of how the hack occurred and how it determined who was impacted, the Everest ransomware group has claimed credit and has begun leaking or selling the data due to STIIIZY failing to respond to them or pay a ransom.[4]

7. Everest has also been known for "acting as initial access brokers, selling access to corporate networks to other threat actors to perform their own attacks." This means that Private Information that Everest gathered from the Data Breach could be sold or used to develop new methods to gain further unauthorized access to STIIIZY's systems.[5] Because STIIIZY has not made clear how it ensures its computer and information technology systems are secure, Plaintiffs reasonably fear that their information, which STIIIZY still has, could be stolen again by cybercriminals due to STIIIZY's security failures.

8. The Data Breach was a direct result of STIIIZY's failure to implement adequate and reasonable cybersecurity procedures and protocols, consistent with industry standards, and necessary to protect Private Information from the foreseeable threat of a cyberattack.

---

[4] *Cannabis company Stiiizy says hackers accessed customers' ID documents* TECHCRUNCH (Jan. 10, 2025), https://techcrunch.com/2025/01/10/cannabis-company-stiiizy-says-hackers-accessed-customers-id-documents/

[5] Lawrence Abrams, *STIIIZY data breach exposes cannabis buyers' IDs and purchases*, BLEEPING COMPUTER (Jan. 10, 2025), https://www.bleepingcomputer.com/news/security/stiiizy-data-breach-exposes-cannabis-buyers-ids-and-purchases/

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

9. By obtaining Plaintiffs' and Class Members' Private Information, Defendant assumed a duty to Plaintiffs and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard their Private Information against unauthorized access and disclosure.

10. The injury to Plaintiffs and Class Members is compounded by the fact that STIIIZY did not immediately notify those affected that their Private Information was subject to unauthorized access and exfiltration. Instead, STIIIZY waited until January 7, 2025, to issue notice on its website, and waited even longer before sending direct notice to the Data Breach victims.

11. STIIIZY's failure to timely notify the victims of its Data Breach prevented Plaintiffs and Class Members from taking swift and affirmative measures to prevent or mitigate the resulting harm, including, but not limited to, changing their passwords and monitoring accounts for unauthorized activity. When Defendant finally issued notice, it downplayed and provided incomplete information about the nature and scope of the breach.

12. This Data Breach was both foreseeable and preventable. Had STIIIZY followed well-established guidance from many government agencies (e.g., the FTC and Government Accountability Office (GAO)) to take simple steps to protect Plaintiffs and Class Members' Private Information—such as enabling multi-factor authentication and access controls, encrypting sensitive data, regularly monitoring systems for suspicious activity, and setting controls against large extractions of data—the Data Breach could have been avoided or prevented .

13. The security of Plaintiffs' and Class Members' identities is at substantial risk because their Private Information is now in the hands of dangerous criminals. This risk will continue for the course of their lives. Defendant exposed Plaintiffs and

Class Members to present and imminent risks of fraud and identity theft. Among other measures, Plaintiffs and Class Members already have and will continue to be forced to closely monitor their financial accounts to guard against identity theft. Armed with the Private Information accessed in the Data Breach, data thieves can commit a wide range of crimes.

14. As a result of STIIIZY's inadequate security and breach of its duties and obligations, Plaintiffs and Class Members have suffered injuries that are a direct and proximate result of those breaches. These injuries include: (i) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their Private Information; (ii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including, but not limited to, lost time; (iii) the continued, long-term, and certain increased risk that unauthorized persons will access and abuse Plaintiffs' and Class Members' Private Information; (iv) the continued and certain increased risk that the Private Information that remains in Defendant's possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake proper measures to protect the Private Information; (v) invasion of privacy and increased risk of fraud and identity theft; (vi) theft of their Private Information and the resulting loss of privacy rights in that information; (vii) diminution in value and/or lost value of Private Information, which is a form of property that Defendant obtained from Plaintiffs and Class Members. This action seeks to remedy these failings and their consequences. Plaintiffs and Class Members have a continuing interest in ensuring that their Private Information is and remains safe, and they should be entitled to injunctive and other equitable relief.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

15. Plaintiffs bring this lawsuit on behalf of themselves and all those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that it collected and maintained. To remedy these violations of law, Plaintiffs and Class Members seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Defendant's data security protocols and employee training practices), reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies this Court deems just and proper.

PARTIES

A. Plaintiffs

1. G.E.

16. G.E. ("Plaintiff G.E.") is a natural person and citizen of San Francisco, California, where he intends to remain.

17. Plaintiff G.E. entrusted his Private Information to Defendant in connection with his purchase of products from Defendant.

18. Prior to the October 2024 Data Breach, Plaintiff G.E. purchased STIIIZY products at its location in Alameda, California – one of the four confirmed locations from which Private Information has been exfiltrated.

19. In order to purchase cannabis from STIIIZY, Plaintiff G.E. was required to, and did, provide a driver's license to a STIIIZY employee, who input a scan of his Driver's License, his name, and other information into STIIIZY's system.

20. Prior to making the purchase and providing STIIIZY with his sensitive information, G.E. viewed and relied on STIIIZY's representations regarding security and privacy, and reasonably believed that his information would be protected.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

21. Prior to making the purchase and providing STIIIZY with his Private Information, Plaintiff G.E. reasonably believed that his information would be protected by STIIIZY and that his sensitive private information would not be disclosed.

22. But for STIIIZY's misrepresentations and omissions regarding the adequacy of its data security measures, Plaintiff G.E. would not have provided his Private Information to Defendant nor would he have transacted with Defendant.

23. At the time of the Data Breach Defendant maintained Plaintiff G.E.'s Private Information in its system, and, on information and belief, said Private Information remains in Defendant's possession.

24. Defendant deprived Plaintiff G.E. of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him.

25. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff G.E.'s Private Information to theft by cybercriminals and sale on the dark web.

26. When Plaintiff G.E.'s Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff G.E. suffered injury from a loss of privacy.

27. Plaintiff G.E. is careful about sharing his Private Information, and takes reasonable steps to protect it. Plaintiff G.E. has never knowingly transmitted unencrypted PII over the internet or through other unsecured means.

28. Plaintiff G.E. is exposed and will continue to be exposed for the remainder of his life, to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties.

29. As a result of the Data Breach, Plaintiff G.E. has spent substantial time attempting to mitigate damages caused by the Data Breach, including monitoring all

of his accounts and financial activity. The time spent dealing with the Data Breach is time Plaintiff G.E. otherwise would have spent on other activities such as work and/or recreation. Plaintiff G.E. anticipates taking additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continuously reviewing his accounts for unauthorized activity. Plaintiff did this at the direction of STIIIZY which directed him to "remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity."[6]

30. As a result of the Data Breach, Plaintiff G.E. has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff G.E. entrusted to Defendant. This information has inherent value that Plaintiff G.E. was deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

31. Plaintiff G.E. has and is continuing to experience significant emotional distress, fear, stress, frustration, and anxiety about potential identity theft and fraudulent activity, because Defendant disclosed his Private Information to unauthorized parties who may now use that information for improper and unlawful purposes. These concerns manifested in physical symptoms, including loss of sleep and decreased appetite.

32. Pursuant to Cal. Civ. Code § 1798.150(b), on or about March 20, 2025, Plaintiff G.E. sent his notice letter by certified mail, return receipt requested, to STIIIZY's principal place of business, notifying STIIIZY of its violations of the

[6] Notice of Data Breach.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

California Consumer Privacy Act ("CCPA") and affording it the opportunity to correct its business practices and rectify the harm it caused.

33. On April 18, 2025, Defendant replied to Plaintiff G.E's letter but failed to provide the relief requested in the letter or fix the injury it caused to Plaintiff G.E. due to the Data Breach.

34. Plaintiff G.E. is also at a continued risk of harm because, on information and belief, his Private Information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and are subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

2. DONALD HATCH

35. Donald Hatch ("Plaintiff Hatch") is a natural person and citizen of California, where he intends to remain.

36. Plaintiff Hatch entrusted his Private Information to Defendant in connection with his purchase of products from Defendant. Plaintiff was a customer of the STIIIZY location on 1528 Webster Ave., Alameda, CA listed in the Notice.

37. Prior to making the purchase and providing STIIIZY with his sensitive Private Information, Plaintiff Hatch reasonably believed that his information would be protected by STIIIZY and that his sensitive and private information would not be disclosed.

38. But for STIIIZY's misrepresentations and omissions regarding the adequacy of its data security measures, Plaintiff Hatch would not have provided his Private Information to Defendant nor would he have transacted with Defendant.

39. Plaintiff Hatch is careful about sharing his Private Information and takes reasonable steps to protect it. Plaintiff Hatch has never knowingly transmitted unencrypted Private Information over the internet or through other unsecured means.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

40. At the time of the Data Breach, Defendant had Plaintiff Hatch's Private Information in its systems, and on information and belief they continue to retain that information.

41. Plaintiff Hatch received the Notice Letter, by email, directly from Defendant, dated January 16, 2024. According to the Notice Letter, Plaintiff Hatch's Private Information was improperly accessed and obtained by unauthorized third parties, including his name, address, date of birth, age, driver's license number, photograph, the signatures appearing on a government ID card, medical cannabis cards, transaction histories, and other personal information.

42. Since receiving the Notice, Plaintiff Hatch made reasonable efforts to mitigate the Data Breach's impact, including, but not limited to, monitoring his various financial and banking accounts for fraudulent activity.

43. Defendant deprived Plaintiff Hatch of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him.

44. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Hatch's Private Information to theft by cybercriminals and sale on the Dark Web.

45. Plaintiff Hatch has, and is continuing to experience, fear, stress, frustration, and anxiety, among other issues, because Defendant disclosed his Private Information to unauthorized parties who may now use that information for improper and unlawful purposes.

46. Plaintiff Hatch is exposed and will continue to be exposed for the remainder of his life to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third-parties and/or cybercriminals.

47. As a result of the Data Breach, Plaintiff Hatch has spent substantial time attempting to mitigate damages caused by the Data Breach, including monitoring all of his accounts and financial activity. The time spent dealing with Defendant's Data Breach is time Plaintiff Hatch otherwise would have spent on other activities such as work and/or recreation. Plaintiff Hatch anticipates taking additional time-consuming and necessary steps to help mitigate the harm caused by the Data Breach, including continuously reviewing his accounts for unauthorized activity. Plaintiff Hatch did this at the direction of STIIIZY which directed individuals to "remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity."[7]

48. As a result of the Data Breach, Plaintiff Hatch has been further injured by the damage to and loss in value of his Private Information—a form of intangible property that Plaintiff Hatch entrusted to Defendant. This information has inherent value that Plaintiff Hatch was deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

49. Pursuant to Cal. Civ. Code§ 1798.150(b), on or about February 10, 2025, Plaintiff Hatch sent his notice letter by certified mail, return receipt requested, to STIIIZY's principal place of business, notifying STIIIZY of its violations of the CCPA and affording it the opportunity to correct its business practices and rectify the harm it caused.

50. On March 12, 2025, Defendant replied to Plaintiff Hatch's letter but failed to provide the relief requested in the letter or fix the injury it caused to Plaintiff Hatch due to the Data Breach.

---

[7] Notice of Data Breach.

51. Plaintiff Hatch is also at a continued risk of harm because, on information and belief, his Private Information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and are subject to further attack so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

3. BRADLEY ANDERSON

52. Plaintiff Bradley Anderson ("Plaintiff Anderson") is a natural person and citizen of California, where he intends to remain.

53. Plaintiff Anderson is also a former employee and customer of STIIIZY.

54. As a condition of employment, Plaintiff Anderson provided Defendant with his Private Information. Defendant used that Private Information to facilitate its employment of Plaintiff, including payroll.

55. Plaintiff Anderson provided his Private Information to Defendant and trusted that the company would use reasonable measures to protect it according to state and federal law.

56. Plaintiff Anderson had entrusted his Private Information to Defendant in connection with his employment by Defendant. Prior to providing STIIIZY with his sensitive Private Information, Plaintiff Anderson reasonably believed that his information would be protected by STIIIZY and that his sensitive private information would not be disclosed.

57. But for STIIIZY's misrepresentations and omissions regarding the adequacy of its data security measures, Plaintiff Anderson would not have provided his Private Information to Defendant.

58. At the time of the Data Breach Defendant maintained Plaintiff Anderson's Private Information in its system.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

59. On information and belief, Plaintiff Anderson's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

60. Defendant deprived Plaintiff Anderson of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him of the Data Breach.

61. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Anderson's Private Information for theft by cybercriminals and sale on the Dark Web.

62. When Plaintiff Anderson's Private Information was accessed and obtained by a third-party without his consent or authorization, Plaintiff Anderson suffered injury from a loss of privacy.

63. Plaintiff Anderson does not recall ever learning that his Private Information was compromised in a data breach incident, other than the Data Breach at issue in this case.

64. As a result of the Data Breach, Plaintiff Anderson has spent time and made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit card and financial account statements, changing his online account passwords, placing a credit freeze through all the three main credit bureaus, and monitoring his credit information.

65. Plaintiff is now subject to the present and continuing risk of fraud, identity theft, and misuse resulting from his Private Information being placed in the hands of unauthorized third parties. This injury was worsened by Defendant's failure to inform Plaintiff about the Data Breach in a timely fashion.

66. Once an individual's Private Information is for sale and accessed on the Dark Web, as Plaintiff's Private Information is here as a result of the Breach,

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

cybercriminals are able to use the stolen and compromised to gather and steal even more information.

67. As a result of the Data Breach, Plaintiff Anderson has been further injured by the damages to and loss in value of his Private Information—a form of intangible property that Plaintiff Anderson entrusted to Defendant. This information has inherent value that Plaintiff Anderson was deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

68. Pursuant to Cal. Civ. Code§ 1798.150(b), on or about January 21, 2025, Plaintiff Anderson sent his notice letter by certified mail, return receipt requested, to STIIIZY's principal place of business, notifying STIIIZY of its violations of the CCPA and affording it the opportunity to correct their business practices and rectify the harm it caused.

69. At the time of this filing, long after Defendant's response was due, Plaintiff Anderson has not received a response from Defendant to his CCPA letter.

70. Plaintiff Anderson is also at a continued risk of harm because, on information and belief, his Private Information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and are subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

4. DANIEL MARTINEZ

71. Plaintiff, Daniel Martinez ("Plaintiff Martinez") is a natural person and citizen of California, where he intends to remain.

72. Plaintiff Martinez had entrusted his Private Information to Defendant in connection with his purchase of products from Defendant.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

73. Prior to making the purchase and providing STIIIZY with his sensitive Private Information, Plaintiff Martinez reasonably believed that his information would be protected by STIIIZY and that his sensitive and private information would not be disclosed.

74. But for STIIIZY's misrepresentations and omissions regarding the adequacy of its data security measures, Plaintiff Martinez would not have provided his Private Information to Defendant, nor would he have transacted with Defendant.

75. At the time of the Data Breach Defendant maintained Plaintiff Martinez's Private Information in its system.

76. Plaintiff Martinez received the Notice Letter, by email, directly from Defendant, dated January 16, 2024. According to the Notice Letter, Plaintiff Martinez's Private Information was improperly accessed and obtained by unauthorized third parties, including his name, address, date of birth, age, drivers' license number, photograph, the signatures appearing on a government ID card, medical cannabis cards, transaction histories, and other personal information.

77. Defendant deprived Plaintiff Martinez of the earliest opportunity to guard himself against the Data Breach's effects by failing to promptly notify him.

78. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff Martinez's Private Information for theft by cybercriminals and sale on the Dark Web.

79. When Plaintiff Martinez's Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Martinez suffered injury from a loss of privacy.

80. Plaintiff Martinez is exposed and will continue to be exposed for the remainder of his life to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his PII being obtained by unauthorized third parties and/or cybercriminals.

81. As a result of this data breach, Plaintiff Martinez has spent substantial time attempting to mitigate damages caused by this data breach, including monitoring all of his accounts and financial activity. The time spent dealing with Defendant's Data Breach is time Plaintiff Martinez otherwise would have spent on other activities such as work and/or recreation. Plaintiff Martinez anticipates taking additional time-consuming and necessary steps to help mitigate the harm caused by the data breach, including continuously reviewing his accounts for unauthorized activity. Plaintiff Martinez did this at the direction of STIIIZY which directed individuals to "remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity."[8]

82. As a result of the Data Breach, Plaintiff Martinez has been further injured by the damage to and loss in value of his Private Information—a form of intangible property that Plaintiff Martinez entrusted to Defendant. This information has inherent value that Plaintiff Martinez was deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

83. Plaintiff Martinez is experiencing anxiety, distress, and fear regarding this Data Breach because Defendant disclosed his Private Information to unauthorized parties who may now use that information for improper and unlawful purposes. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

84. Pursuant to Cal. Civ. Code§ 1798.150(b), on or about January 21, 2025, Plaintiff Martinez sent his notice letter by certified mail, return receipt requested, to STIIIZY's principal place of business, notifying STIIIZY of its violations of the

[8] Notice of Data Breach.

CCPA and affording it the opportunity to correct their business practices and rectify the harm it caused.

85. On February 20, 2025, Defendant replied to Plaintiff Martinez's letter but failed to provide the relief requested in the letter or fix the injury it caused to Plaintiff Martinez due to the Data Breach.

86. Plaintiff Martinez is also at a continued risk of harm because, on information and belief, his Private Information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and are subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

5. LORENZO MONTOYA

87. Plaintiff Lorenzo Montoya ("Plaintiff Montoya") is a natural person and citizen of California, where he intends to remain.

88. Plaintiff Montoya had entrusted his Private Information to Defendant in connection with his purchase of products from Defendant.

89. Prior to making the purchase and providing STIIIZY with his sensitive information, Plaintiff Montoya reasonably believed that his information would be protected by STIIIZY and that his sensitive and private information would not be disclosed.

90. But for STIIIZY's misrepresentations and omissions regarding the adequacy of its data security measures, Plaintiff Montoya would not have provided his Private Information to Defendant, nor would he have transacted with Defendant.

91. At the time of the Data Breach—October 10, 2024, through November 10, 2024—Defendant maintained Plaintiff Montoya's Private Information in its system.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

92. Plaintiff Montoya received the Notice Letter, by email, directly from Defendant, dated January 16, 2024. According to the Notice Letter, Plaintiff Montoya's PII was improperly accessed and obtained by unauthorized third parties, including his name, address, date of birth, age, driver's license number, photograph, the signatures appearing on a government ID card, medical cannabis cards, transaction histories, and other personal information.

93. When Plaintiff Montoya's Private Information was accessed and obtained by a third party without his consent or authorization, Plaintiff Montoya suffered injury from a loss of privacy.

94. Plaintiff Montoya is exposed and will continue to be exposed for the remainder of his life to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from his Private Information being obtained by unauthorized third parties and/or cybercriminals.

95. As a result of the Data Breach, Plaintiff Montoya has spent substantial time attempting to mitigate damages caused by this data breach. The time spent dealing with Defendant's Data Breach is valuable time Plaintiff Montoya otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff Montoya did this at the direction of Defendant's Notice Letter, which instructed individuals to "remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity."[9]

96. As a result of the Data Breach, Plaintiff Montoya has been further injured by the damages to and loss in value of his Private Information—a form of intangible

[9] Notice of Data Breach.

property that Plaintiff Montoya entrusted to Defendant. This information has inherent value that Plaintiff Montoya was deprived of when his Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

97. Pursuant to Cal. Civ. Code§ 1798.150(b), on or about January 18, 2025, Plaintiff Montoya sent his notice letter by certified mail, return receipt requested, to STIIIZY's principal place of business, notifying STIIIZY of its violations of the CCPA and affording it the opportunity to correct their business practices and rectify the harm it caused. STIIIZY responded by letter on March 7, 2025, denying the CCPA applies and ultimately failing to cure its violations of the statute.

98. Plaintiff Montoya is also at a continued risk of harm because, on information and belief, his Private Information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and are subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

6. ELIZABETH OROZCO-PREZA

99. Plaintiff Elizabeth Orozco-Preza ("Plaintiff Orozco-Preza") is a natural person and citizen of California, where she intends to remain.

100. Plaintiff Orozco-Preza had entrusted her Private Information to Defendant in connection with her purchase of products from Defendant.

101. Prior to making the purchase and providing STIIIZY with her sensitive Private Information, Plaintiff Orozco-Preza reasonably believed that her information would be protected by STIIIZY and that her sensitive and private information would not be disclosed.

102. But for STIIIZY's misrepresentations and omissions regarding the adequacy of its data security measures, Plaintiff Orozco-Preza would not have

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

provided her Private Information to Defendant, nor would she have transacted with Defendant.

103. At the time of the Data Breach Defendant maintained Plaintiff Orozco-Preza's Private Information in its system.

104. Plaintiff Orozco-Preza is very careful about sharing her sensitive PII. She stores any documents containing her Private Information in a safe and secure location. Plaintiff Orozco-Preza has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Plaintiff Orozco-Preza would not have entrusted her Private Information to Defendant had she known of Defendant's lax data security policies.

105. Plaintiff Orozco-Preza received the Notice Letter, by email, directly from Defendant, dated January 8, 2024. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including her name, address, date of birth, age, driver's license number, passport number, photograph, the signatures appearing on a government ID card, medical cannabis cards, transaction histories, and other personal information.

106. When Plaintiff Orozco-Preza's Private Information was accessed and obtained by a third party without her consent or authorization, Plaintiff Orozco-Preza suffered injury from a loss of privacy.

107. Plaintiff Orozco-Preza is exposed and will continue to be exposed for the remainder of her life to imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse proximately resulting from her Private Information being obtained by unauthorized third parties and/or cybercriminals.

108. As a result of the Data Breach, Plaintiff Orozco-Preza has spent substantial time attempting to mitigate damages caused by this data breach, including

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

by researching and verifying the legitimacy of the Data Breach. The time spent dealing with Defendant's Data Breach is valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured. Plaintiff Orozco-Preza did this at the direction of Defendant's Notice Letter, which instructed individuals to "remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity."[10]

109. The Data Breach has caused Plaintiff Orozco-Preza to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant has still not fully informed her of key details about the Data Breach's occurrence.

110. As a result of the Data Breach, Plaintiff Orozco-Preza has been further injured by the damage to and loss in value of her Private Information—a form of intangible property that Plaintiff Orozco-Preza entrusted to Defendant. This information has inherent value that Plaintiff Orozco-Preza was deprived of when her Private Information was negligently made accessible to and intentionally and maliciously exfiltrated by cybercriminals.

111. Pursuant to Cal. Civ. Code§ 1798.150(b), on or about February 3, 2025, Plaintiff Orozco-Preza sent her notice letter by certified mail, return receipt requested, to STIIIZY's principal place of business, notifying STIIIZY of its violations of the CCPA and affording it the opportunity to correct their business practices and rectify the harm it caused.

112. On February 21, 2025, Defendant replied to Plaintiff Orozco-Preza's letter but failed to provide the relief requested in the letter or fix the injury it caused to Plaintiff Orozco-Preza due to the Data Breach.

[10] Notice of Data Breach.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

113. Plaintiff Orozco-Preza is also at a continued risk of harm because, on information and belief, her Private Information remains in Defendant's systems, which have already been shown to be susceptible to compromise and attack, and are subject to further attack, so long as Defendant fails to undertake the necessary and appropriate data security measures to protect the Private Information in its possession.

B. Defendant

STIIIZY Inc.

114. Defendant STIIIZY, Inc. is incorporated in Delaware, with its principal place of business in the city of Los Angeles, California. Defendant conducts business, selling cannabis products to customers throughout the states of California, Washington, Nevada, Michigan, and Arizona.

JURISDICTION AND VENUE

115. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than one hundred (100) putative Class Members defined below, and minimal diversity exists because at least one Plaintiff is a citizen of a state different from the citizenship of Defendant. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. § 1367.

116. This Court has personal jurisdiction over Defendant because Defendant's principal place of business is in this District.

117. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events or omissions giving rise to the claims occurred in this district – this is where Defendant's principal place of business is located and conducts substantial business, including its actions and inactions leading to the data

breach at issue. Defendant also gains revenue and profits from doing business in this District.

FACTUAL ALLEGATIONS

118. STIIIZY is a retailer of cannabis with hundreds of thousands of customers primarily in California, but also across the country. Defendant collects and processes the personal data of its customers. To purchase products from Defendant, customers are forced to entrust Defendant with their Private Information.

119. The information collected and stored by Defendant includes, but is not limited to, ***names, addresses, dates of birth, driver's license numbers, passport numbers, photographs, the signatures appearing on government ID cards, and medical cannabis cards***.

120. Defendant additionally has claimed that the Data Breach only impacted consumer profiles associated with the following STIIIZY locations:

- STIIIZY Union Square: 180 O'Farrell Street, San Francisco, CA
- STIIIZY Mission: 3326 Mission Street, San Francisco, CA
- STIIIZY Alameda: 1528 Webster St., Alameda, CA
- STIIIZY Modesto: 426 McHenry Ave., Modesto, CA.[11]

121. Defendant holds itself as a company that prioritizes customers' privacy and cyber security, and has repeatedly assured its customers that it "implements security measures designed to protect your information from unauthorized access, disclosure or accidental loss or destruction."[12]

122. Defendant is aware of its commitments, warranting that it "utilize[s] appropriate physical, technical and managerial safeguards designed to protect the

---

[11] Notice of Data Breach.

[12] *Privacy Policy*, STIIIZY, https://www.stiiizy.com/policies/privacy-policy (May 20, 2025).

information we collect."[13] Because the Defendant collects, handles, and stores highly sensitive information - passports, driver's licenses, medical cards, social security numbers, dates of birth, and more – robust and industry appropriate security measures were required here, such as complete vetting of vendor security practices, use of multi-factor authentication, complete and immediate patching of all software and servers, and consistent and real-time threat detection. Defendant's failure to do so directly enabled the hackers to extract the sensitive Private Information, causing this Data Breach.

123. Plaintiffs and other similarly situated customers relied to their detriment on Defendant's uniform representations and omissions regarding data security, including Defendant's failure to alert customers that its security protections were inadequate, and that Defendant would forever store Plaintiffs' and Class Members' Private Information, failing to archive it, protect it, or at the very minimum warn consumers of the anticipated and foreseeable data breach.

124. Plaintiffs and other similarly situated customers trusted Defendant with their sensitive and valuable Private Information. If Defendant disclosed to Plaintiffs and its other customers that its data systems were not secure and were vulnerable to attack, Plaintiffs would not have done business with Defendant or provided it with their Private Information.

A. The Data Breach

125. At all relevant times, STIIIZY failed to maintain proper security measures despite its promises of safety and security to consumers and its common law and statutory duties to safeguard personal information from unauthorized access.

126. On November 20, 2024, Defendant was notified by a vendor of point-of-sale processing services for some of its retail locations that accounts with its

---

[13] *Id.*

organization had been compromised by an organized cybercrime group. Defendant did not notify its customers then, nor make any announcements to alert them of this major security issue. Specifically, an investigation conducted by the vendor revealed that personal information relating to certain STIIIZY customers processed by the vendor was acquired by the threat actors at some point between October 10, 2024 - November 10, 2024. Despite being informed of the cyberattack on November 20, 2024, Defendant kept silent and chose not to notify the affected customers for several months.[14]

127. While STIIIZY initially pointed to the hack as a point-of-service failure, it is actually likely that the hack occurred by cybercriminals breaching the cloud-based software systems where the POS information was stored. This means that STIIIZY failed to properly verify that its vendor was using secure software, and additionally failed to ensure account security on its end by failing to implement essential and adequate security protocols of its cloud-based software or computer system–such as multi-factor authentication, role-based permissions, and sessions monitoring. Additionally, STIIIZY failed to ensure complete encryption of the stored data as well as regular deletion and purging of data no longer necessary, and anomaly detection–leaving the system vulnerable and open to unauthorized and undetected intrusion.

128. On or around January 7, 2025, Defendant finally began notifying some customers of the Data Breach via a posting on its website, including Plaintiffs, when nearly two months had passed since Defendant learned of the unauthorized access.[15]

---

[14] Lawrence Abrams, *STIIIZY data breach exposes cannabis buyers' IDs and purchases*, BLEEPING COMPUTER (Jan. 10, 2025), https://www.bleepingcomputer.com/news/security/stiiizy-data-breach-exposes-cannabis-buyers-ids-and-purchases/.

[15] Notice of Data Breach.

129. Defendant failed to provide actual notice to all individuals who were impacted by the data breach, instead, it posted a notice on its website that does not provide a full and clear explanation of the Data Breach and downplays its significance. This notice states in relevant part (the "Notice"):

> **What Happened?**
>
> On November 20, 2024, we were notified by a vendor of point-of-sale processing services for some of our retail locations that accounts with their organization had been compromised by an organized cybercrime group. An investigation conducted by the vendor revealed that personal information relating to certain STIIIZY customers processed by the vendor was acquired by the threat actors on or around October 10, 2024 - November 10, 2024. Upon receiving notice of the incident, we launched our own investigation to assess the extent of the impact. We have determined that certain of our customers' personal information and documents was acquired by the threat actors. We have been working closely with the vendor and our legal counsel to address the situation, including to determine the cause of the incident. This notification was not delayed by law enforcement.
>
> **What Information Was Involved?**
>
> Based on our initial investigation, the incident only impacted consumer profiles associated with the following STIIIZY locations:
>
> - STIIIZY Union Square: 180 O'Farrell Street, San Francisco, CA
> - STIIIZY Mission: 3326 Mission Street, San Francisco, CA
> - STIIIZY Alameda: 1528 Webster St., Alameda, CA
> - Authentic 209: 426 McHenry Ave., Modesto, CA
>
> The incident impacted information contained on government-issued identification cards, including drivers' licenses and medical cannabis cards, as well as information related to transactions with our dispensaries. The categories of information compromised include name, address, date of birth, age, drivers' license number, passport number, photograph, the signatures appearing on a government ID card, medical cannabis cards, transaction histories, and other personal information. Not all of this

information was affected for each impacted individual.[16]

130. In its initial statement, Defendant did not disclose how many customers' Private Information was breached from each location, leaving many customers to speculate whether their information compromised. Defendant also downplayed the extent of the Data Breach, and the likely harm affected victims may experience. Additionally, while Defendant obtained scans of driver's licenses and medical cannabis cards and retained such information in their systems, they did not necessarily have current contact information for all customers. Thus, it is almost guaranteed that not all victims of the Data Breach have received actual notice.

B. Everest leaked—and then flooded—the Dark Web with the stolen Private Information.

131. The Everest ransomware group, the culprit behind this hack, has long been known for targeting entities with highly sensitive information, like Defendant, and using ransomware to make businesses' computer systems inaccessible as well as stealing data to leak and sell if the ransom is not paid. Here, Defendant could have prevented this breach though improved security procedures, access controls like multi-factor authentication, strong password and authentication policies for remote access, conducting regular tabletop and training exercises with all employees, consistent and real-time monitoring of computer access and logs, limiting and disabling internet facing information, encryption of all sensitive information, and deleting and purging information that is no longer necessary. If Defendant had proper and adequate policies to ensure that its system was secure, it would have prevented the Data Breach. Defendant chose not to spend time and resources protecting its customers' Private Information, directly leading to the Data Breach.

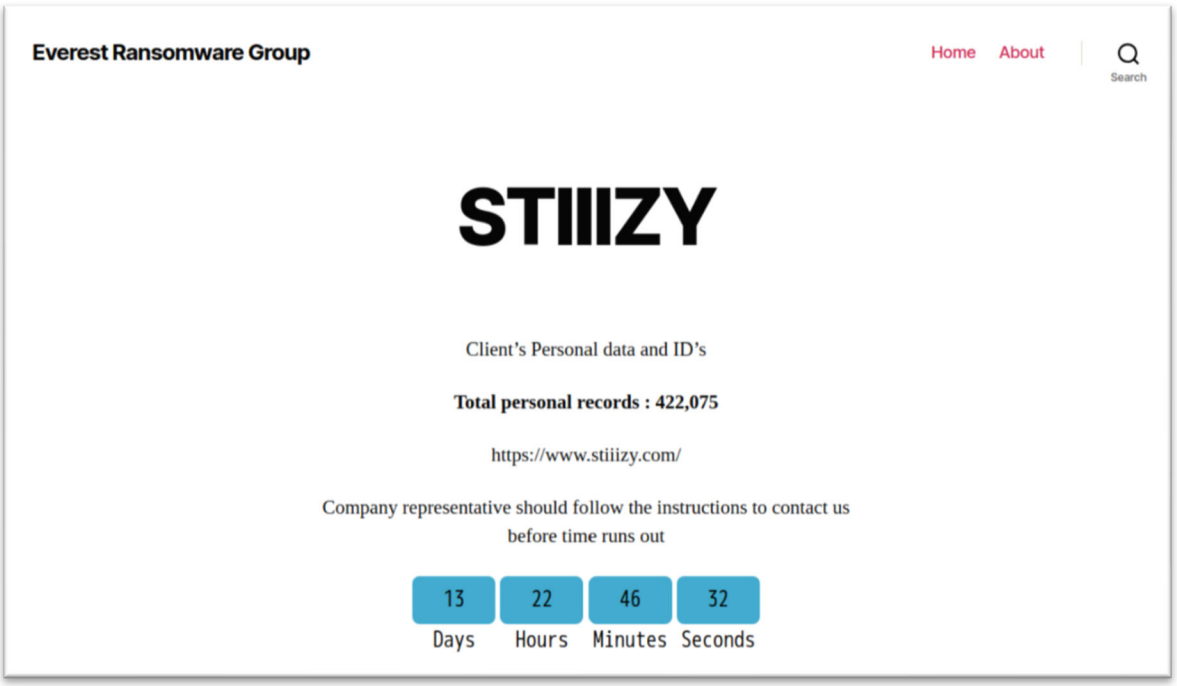
---

[16] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

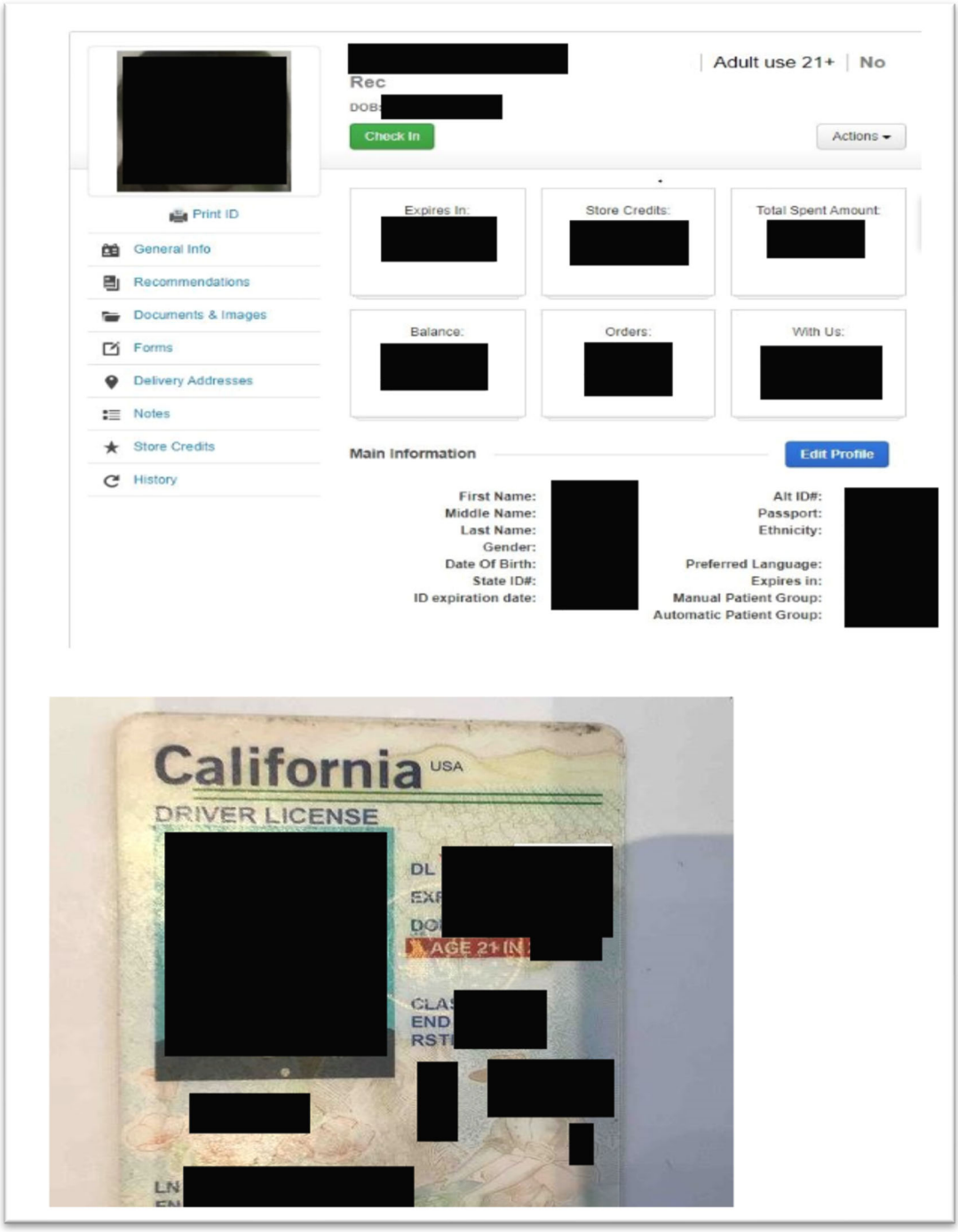
Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

132. On or around November 24, 2024, Everest posted information about Defendant on the Dark Web—revealing that it had obtained "Client's Personal data and ID's" and "Total personal records : 422,075[.]"[17] Everest warned that "Company representative should follow the instructions to contact us before time runs out[.]"[18] To that end, Everest also included a countdown timer which indicated that Everest would leak the stolen Private Information in 13 days, 22 hours, 46 minutes, and 32 seconds.[19] Further, Everest proved that it had stolen Private Information by publishing numerous screenshots of Class Members' Private Information—which included, two California driver licenses, screenshots of customer profiles, a Medical Recommendation for medical marijuana use, screenshots of file lists, a Romanian



[17] *Everest*, RANSOMLOOK (Nov. 24, 2024) https://www.ransomlook.io/group/everest.
[18] *Id.*
[19] *Id.*

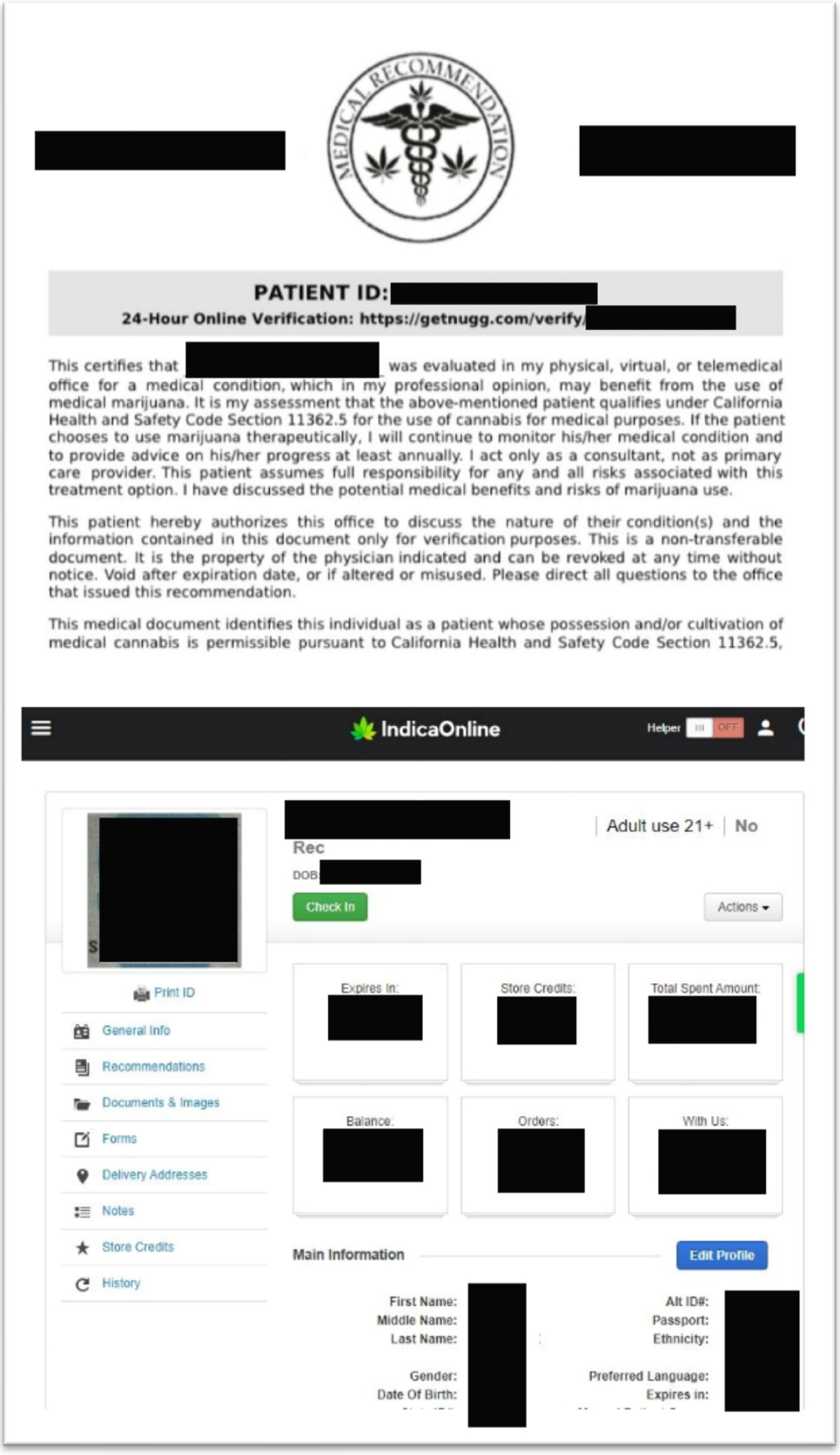
passport, and a California medical cannabis card.[20] Screenshots of Everest's post on the Dark Web are provided below (with redactions as necessary).[21]



[20] *Id.*

[21] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265



[redacted]

MEDICAL RECOMMENDATION

[redacted]

PATIENT ID: [redacted]

24-Hour Online Verification: https://getnugg.com/verify/[redacted]

This certifies that [redacted] was evaluated in my physical, virtual, or telemedical office for a medical condition, which in my professional opinion, may benefit from the use of medical marijuana. It is my assessment that the above-mentioned patient qualifies under California Health and Safety Code Section 11362.5 for the use of cannabis for medical purposes. If the patient chooses to use marijuana therapeutically, I will continue to monitor his/her medical condition and to provide advice on his/her progress at least annually. I act only as a consultant, not as primary care provider. This patient assumes full responsibility for any and all risks associated with this treatment option. I have discussed the potential medical benefits and risks of marijuana use.

This patient hereby authorizes this office to discuss the nature of their condition(s) and the information contained in this document only for verification purposes. This is a non-transferable document. It is the property of the physician indicated and can be revoked at any time without notice. Void after expiration date, or if altered or misused. Please direct all questions to the office that issued this recommendation.

This medical document identifies this individual as a patient whose possession and/or cultivation of medical cannabis is permissible pursuant to California Health and Safety Code Section 11362.5,

IndicaOnline

Helper

[redacted]

Adult use 21+ | No

Rec

DOB: [redacted]

Check In

Actions

Print ID

General Info

Recommendations

Documents & Images

Forms

Delivery Addresses

Notes

Store Credits

History

Expires In: [redacted]

Store Credits: [redacted]

Total Spent Amount: [redacted]

Balance: [redacted]

Orders: [redacted]

With Us: [redacted]

Main Information

Edit Profile

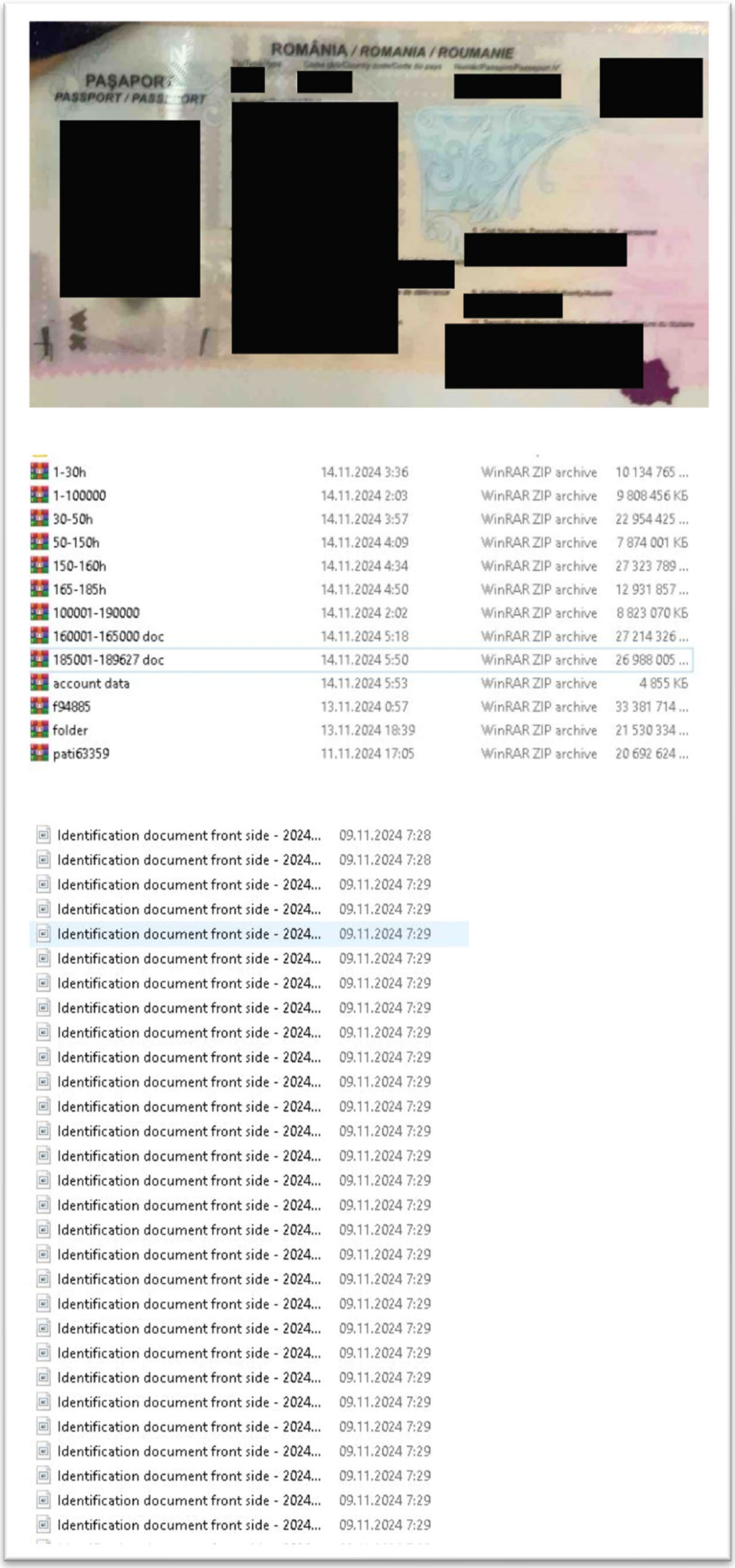
First Name: [redacted]
Middle Name:
Last Name:

Gender:
Date Of Birth:

Alt ID#:
Passport:
Ethnicity:

Preferred Language:
Expires in:

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265



Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

rec - 2024-11-05T011538.774	05.11.2024 4:15
rec - 2024-11-05T011550.402	05.11.2024 4:15
rec - 2024-11-05T011756.869	05.11.2024 4:17
rec - 2024-11-05T011916.767	05.11.2024 4:19
rec - 2024-11-05T012118.818	05.11.2024 4:21
rec - 2024-11-05T012150.024	05.11.2024 4:21
rec - 2024-11-05T012359.574	05.11.2024 4:23
rec - 2024-11-05T012404.149	05.11.2024 4:24
rec - 2024-11-05T012419.433	05.11.2024 4:24
rec - 2024-11-05T012505.039	05.11.2024 4:25
rec - 2024-11-05T012522.838	05.11.2024 4:25
rec - 2024-11-05T012735.181	05.11.2024 4:27
rec - 2024-11-05T012809.815	05.11.2024 4:28
rec - 2024-11-05T012834.952	05.11.2024 4:28
rec - 2024-11-05T012851.975	05.11.2024 4:28
rec - 2024-11-05T012904.040	05.11.2024 4:29
rec - 2024-11-05T012937.255	05.11.2024 4:29
rec - 2024-11-05T013027.596	05.11.2024 4:30
rec - 2024-11-05T013116.026	05.11.2024 4:31
rec - 2024-11-05T013205.593	05.11.2024 4:32
rec - 2024-11-05T013354.993	05.11.2024 4:33
rec - 2024-11-05T013427.432	05.11.2024 4:34
rec - 2024-11-05T013524.053	05.11.2024 4:35
rec - 2024-11-05T013534.353	05.11.2024 4:35
rec - 2024-11-05T013805.344	05.11.2024 4:38
rec - 2024-11-05T013845.591	05.11.2024 4:38
rec - 2024-11-05T013905.695	05.11.2024 4:39
rec - 2024-11-05T014029.595	05.11.2024 4:40
rec - 2024-11-05T014754.546	05.11.2024 4:47

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

133. On or around December 23, 2024, Everest leaked another portion of the stolen Private Information on the Dark Web—stating "STIIIZY Pre-Christmas publication The first part of Christmas 'gifts' for the company. If we continue to be ignored, the amount of published data will only grow. If you do not want to solve this problem with us, then we will cause many times more financial and reputational damage."[22] Therein, Everest published two links such that other cybercriminals could access, download, and misuse the stolen Private Information.[23] A screenshot (with redactions) of the Dark Web post is provided below.[24]

134. On or around December 25, 2024, Everest leaked another portion of the stolen Private Information on the Dark Web—stating "STIIIZY Happy New 20025! More gifts for STIIIZY are on the way At 10 pm, if the company does not contact us

---

[22] *Everest*, RANSOMLOOK (Dec. 23, 2024) https://www.ransomlook.io/group/everest.
[23] *Id.*
[24] *Id.*

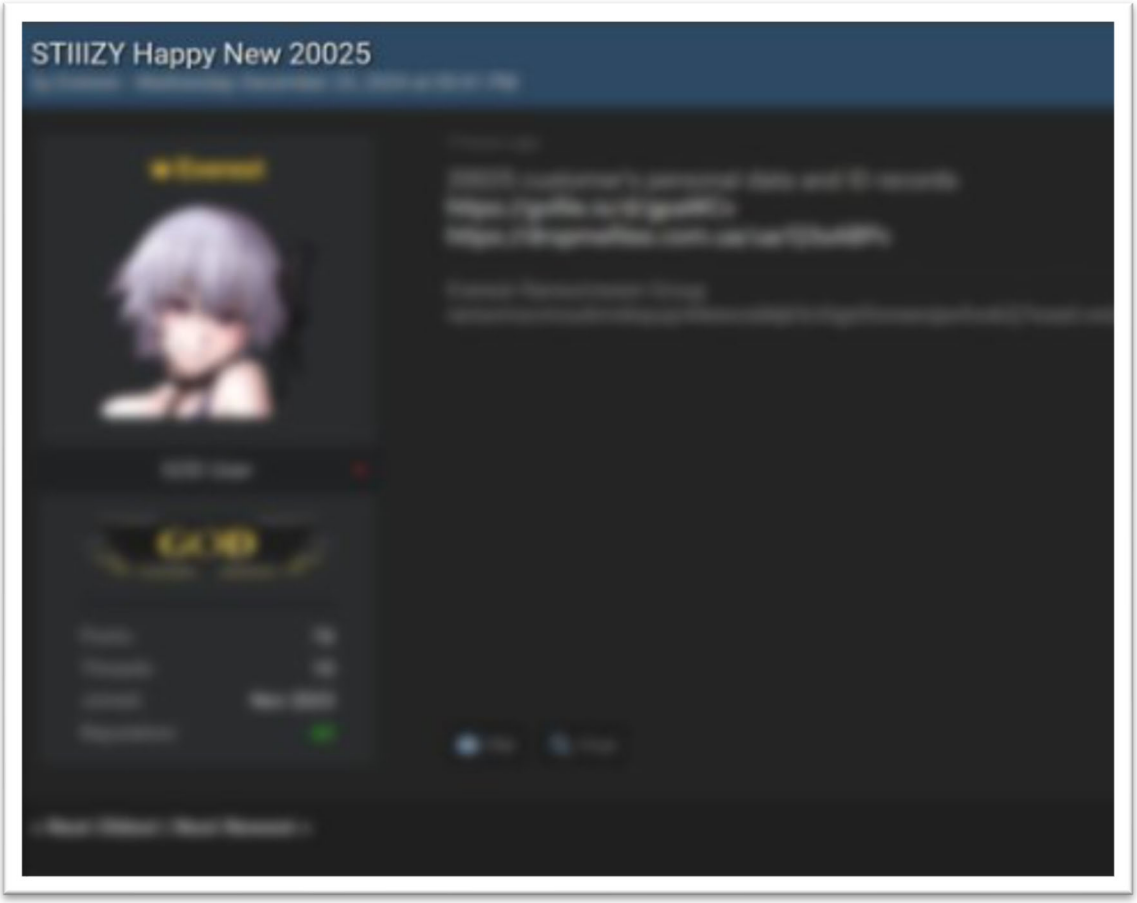
before by any method, we will post another 20025 customer's personal data and ID records . UnMerry Christmas and UnHappy New Year."[25] Therein, Everest published another two links such that other cybercriminals could access, download, and misuse the stolen Private Information.[26] A screenshot (with redactions) of the Dark Web post is provided below.[27]

135. To make matters worse, on December 25, 2024, another cybercriminal group appears to have shared and disseminated the portion of stolen Private Information—that Everest leaked on December 25, 2024—on a different website on the Dark Web.[28] A blurred screenshot of the Dark Web post is provided below.[29]

---

[25] *Everest*, RANSOMLOOK (Dec. 25, 2024) https://www.ransomlook.io/group/everest.
[26] *Id*.
[27] *Id*.
[28] *Dark Web Intelligence* (*@DailyDarkWeb*), X (Dec. 25, 2024, 2:58 PM) https://x.com/DailyDarkWeb/status/1872024061859275029.
[29] *Id*

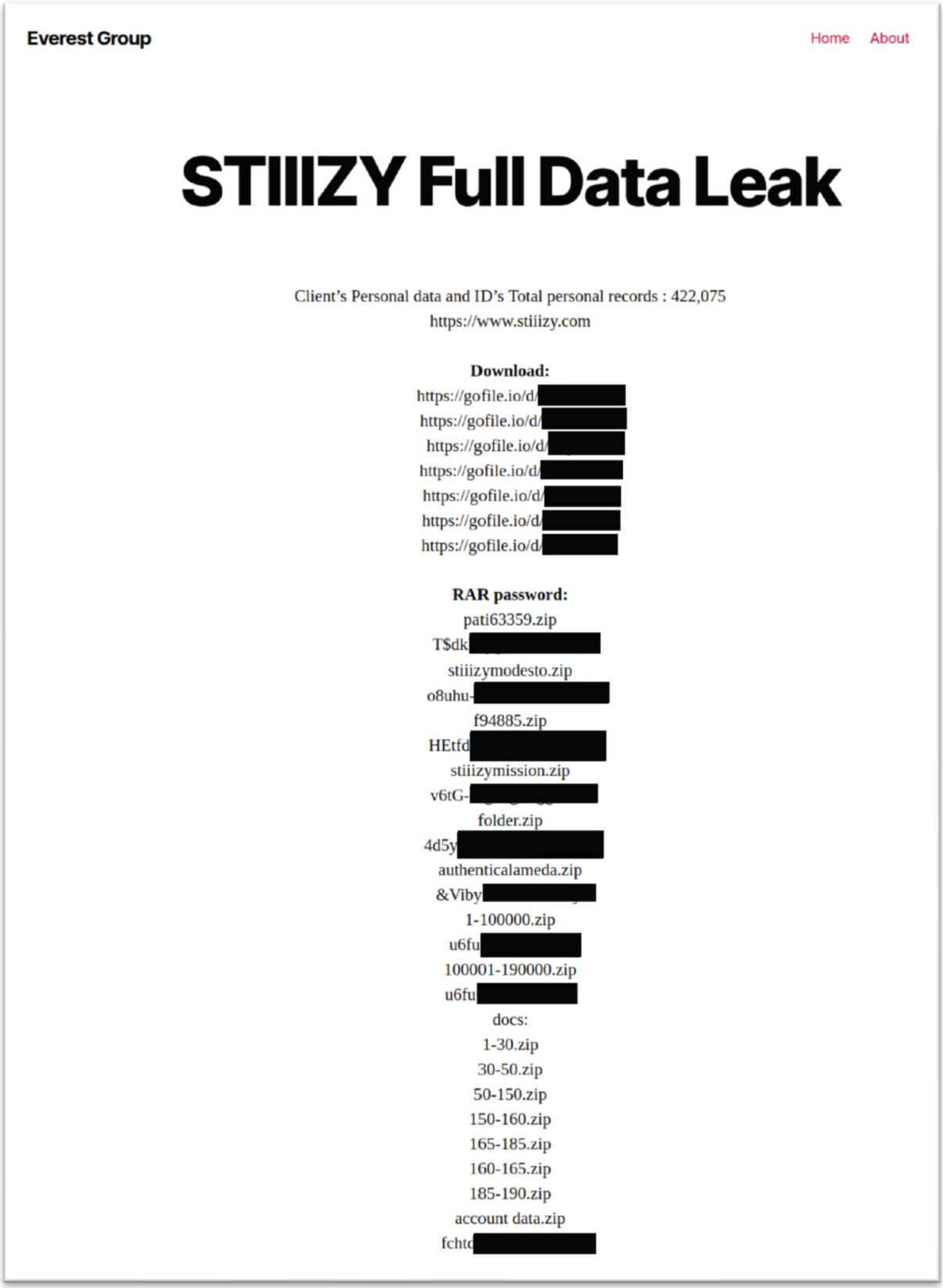
Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265



136. On or around February 12, 2025, Everest leaked the ***full amount*** of stolen Private Information (i.e., 422,075 records of Plaintiffs and Class Members) on the Dark Web—stating "STIIIZY Full Data Leak" and providing seven (7) links and related passwords such that other cybercriminals could access, download, and misuse the stolen Private Information.[30] A screenshot (with redactions) of the Dark Web post is provided below.[31]

[30] *Everest*, RANSOMLOOK (Feb. 12, 2025) https://www.ransomlook.io/group/everest.
[31] *Id*.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265



Everest Group

Home About

STIIIZY Full Data Leak

Client's Personal data and ID's Total personal records : 422,075

https://www.stiizy.com

Download:

https://gofile.io/d/[redacted]

https://gofile.io/d/[redacted]

https://gofile.io/d/[redacted]

https://gofile.io/d/[redacted]

https://gofile.io/d/[redacted]

https://gofile.io/d/[redacted]

https://gofile.io/d/[redacted]

RAR password:

pati63359.zip

T$dk[redacted]

stiizymodesto.zip

o8uhu-[redacted]

f94885.zip

HEtfd[redacted]

stiizymission.zip

v6tG-[redacted]

folder.zip

4d5y[redacted]

authenticalameda.zip

&Viby[redacted]

1-100000.zip

u6fu[redacted]

100001-190000.zip

u6fu[redacted]

docs:

1-30.zip

30-50.zip

50-150.zip

150-160.zip

165-185.zip

160-165.zip

185-190.zip

account data.zip

fchtc[redacted]

137. Despite this public evidence of broad misuse, Defendant failed to warn Plaintiffs and Class Members that the cybercriminal group "Everest" had acquired their Private Information and then ***leaked*** their Private Information on the Dark Web.

138. Indeed, Defendant failed to include—or knowingly omitted—these worrying facts in its Data Breach notice. And in doing so, Defendant misled Plaintiffs and Class Members regarding the severity of the Data Breach.

C. Data Breaches and the Market for Private Information

139. In today's digital economy, "a new form of black gold has emerged, one that is intangible yet infinitely more powerful: data."[32] Personal data has become a "precious commodity," at the forefront of technological innovation.[33] Data is a pivotal economic asset and form of capital, allowing companies rich in it to drive competition. Considering the implications of "big data" in corporate America and the consequences of cyber thefts, which include heavy prison sentences, the value of data is axiomatic. Even this obvious risk-to-reward analysis illustrates beyond doubt that personal information has considerable market value.

140. In a consumer-driven world, the ability to capture and use consumer data to shape products, solutions, and the buying experience is critically important to a business's success.[34] Research shows that organizations that "leverage customer behavior insights outperform peers by 85 percent in sales growth and more than 25

---

[32] Lawrence Teixeira, *The New Black Gold: How Data Became the Most Valuable Asset in Tech*, MEDIUM (Feb 12, 2024), https://medium.com/@lawrenceteixeira/the-new-black-gold-how-data-became-the-most-valuable-asset-in-tech-9e4541262ddf#.

[33] *Id.*

[34] Laci Loew, *Data Differentiation: Why Consumer Data Is A Modern Organization's Real Competitive Advantage*, FORBES (October 2, 2024), https://www.forbes.com/councils/forbescommunicationscouncil/2024/10/02/data-differentiation-why-customer-data-is-a-modern-organizations-real-competitive-advantage/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

percent in gross margin"[35] and that "[d]ata-driven companies are 23 times more likely to top their competitors in customer acquisition, about 19 times more likely to stay profitable and nearly seven times more likely to retain customers."[36]

141. Indeed, an entire economy exists related to the value of personal data. In 2023, the big data technology market was valued at roughly $349 billion, and that value is expected to grow from roughly $397 billion in 2024 to $1,194 billion by 2032.[37]

142. Consumer concern about how companies use their data is on the rise. According to Pew Research, 81% of U.S. adults are concerned about how companies use the data they collect about them.[38] Consumers increasingly say they don't understand what companies are doing with their data, with 67% of U.S. adults saying they understand little to nothing about what companies are doing with their personal data, up from 59% in 2019.[39]

---

[35] Brad Brown, Kumar Kanagasabai, Prashant Pant & Goncalo Serpa Pinto, *Capturing value from your customer data*, MCKINSEY (Mar. 15, 2017), https://www.mckinsey.com/business-functions/quantumblack/our-insights/capturing-value-from-your-customer-data.

[36] Laci Loew, *Data Differentiation: Why Consumer Data Is A Modern Organization's Real Competitive Advantage*, FORBES (October 2, 2024), https://www.forbes.com/councils/forbescommunicationscouncil/2024/10/02/data-differentiation-why-customer-data-is-a-modern-organizations-real-competitive-advantage/.

[37] *Big Data Technology Market Size, Share & Industry Analysis*, FORTUNE BUSINESS INSIGHTS (Jan. 2025), https://www.fortunebusinessinsights.com/industry-reports/big-data-technology-market-100144.

[38] *How Americans View Data Privacy,* PEW RESEARCH CENTER (Oct. 18, 2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/; *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[39] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

143. When a victim's data is compromised in a breach, the victim is exposed to serious ramifications regardless of the sensitivity of the data, including, but not limited to, identity theft, fraud, decline in credit, inability to access healthcare, as well as legal consequences.[40]

144. The U.S. Department of Justice's Bureau of Justice Statistics has found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that resolution of those problems could take more than a year.[41] Indeed, data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.

145. The U.S. Government Accountability Office (GAO) has concluded that it is common for data thieves to hold onto stolen data for extended periods of time before utilizing it for identity theft.[42] In the same report, the GAO noted that while credit monitoring services can assist with detecting fraud, those services do not stop it.[43]

146. As the FTC recognizes, identity thieves can use this information to commit an array of crimes including identity theft, and financial fraud.[44] Indeed, a robust "cyber black market" exists, in which criminals openly post stolen PII on multiple underground Internet websites, commonly referred to as the "dark web."

---

[40] *Data Breach Response: A Guide for Business*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business.

[41] *Victims of Identity Theft*, U.S. DEPARTMENT OF JUSTICE, (Sept. 2015), http://www.bjs.gov/content/pub/pdf/vit14.pdf.

[42] *Data Breaches – Range of Consumer Risks Highlights Limitations of Identity Theft Services*, U.S. GOVERNMENT ACCOUNTABILITY OFFICE, https://www.gao.gov/assets/700/697985.pdf.

[43] *Id.*

[44] *What To Know About Identity Theft*, FEDERAL TRADE COMMISSION, https://consumer.ftc.gov/articles/what-know-about-identity-theft.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

147. Further, criminals often trade stolen PII and PHI on the "cyber black market" or "dark web" for years following a breach. Cybercriminals can, and do, post stolen PII and PHI on the internet, thereby making such information publicly available.

148. When companies entrusted with personal data fail to implement industry best practices, cyberattacks and other data exploitations can go undetected for long periods of time. This worsens the ramifications and can even render the harm irreparable.

149. PII and PHI are valuable commodities for which a black market exists on the dark web, among other places. Personal data can be worth from $1,000 or more on the dark web and the legitimate data brokerage industry is valued at more than $250 billion.

150. In this black market, criminals seek to sell the spoils of their cyberattacks to identity thieves who desire the data to extort and harass victims, take over victims' identities in order to open financial accounts, and otherwise engage in illegal financial transactions under the victims' names.

151. PII and PHI have a distinct, high value—which is why legitimate companies and criminals seek to obtain and sell it. As alleged in more detail below, there is a growing market for individuals' data.[45]

152. Defendant knew or should have known that Plaintiffs' and Class Members' Private Information is valuable, both to legitimate entities, like Defendant, and to cybercriminals.

[45] Emily Wilson, *The Worrying Trend of Children's Data Being Sold on the Dark Web*, TNW (Feb. 23, 2019), https://thenextweb.com/news/children-data-sold-the-dark-web.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

153. Defendant knew or should have known that Plaintiffs and Class Members would reasonably rely upon and trust Defendant's promises regarding security and safety of its data and systems, and that their valuable Private Information would be protected.

D. Defendant failed its duty to comply with FTC Guidelines

154. Defendant collects, receives, and utilizes its customers' extensive PII and PHI.

155. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses that highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

156. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. These guidelines note that businesses should protect the personal information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[46]

157. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data

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

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

being transmitted from the system, and have a response plan ready in the event of a breach.[47]

158. The FTC further recommends that companies not maintain Private Information longer than is needed for the authorization of a transaction, limit access to sensitive data, and require complex passwords to be used on networks. The FTC also advises that businesses use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.

159. In August 2023, the FTC released its publication, Start with Security: A Guide for Business, which sets out ten guideposts for businesses and executives to enhance their companies' security. These lessons are informed by the enforcement actions the FTC has brought against businesses for alleged lapses in security.[48]

160. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumers' private data, treating the failure to employ 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.

161. Section 5 of the FTC Act, 15 U.S.C. § 45, 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

---

[47] *Id.*

[48] *Start with Security: A Guide for Business*, FEDERAL TRADE COMMISSION (2023), available at https://www.bulkorder.ftc.gov/sites/bulkorder.ftc.gov/files/publications/920a_start_with_security_en_aug2023_508_final.pdf.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

162. Defendant failed to properly implement adequate data security practices, despite having actual knowledge of the prevalence of data breaches and the need to properly secure its computer systems. Even though Defendant knew or should have known of the likelihood of a breach if it failed to properly secure its computer systems, it still failed to do so, being the proximate cause of the Data Breach.

163. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the Private Information of its customers or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

164. Upon information and belief, STIIIZY was, at all times, fully aware of its obligation to protect the Private Information of its customers, STIIIZY was also aware of the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of the immense damage that would result to Plaintiffs and the Class.

E. Impact of the Data Breach on Consumers

165. Plaintiffs and the Class have suffered actual harm as a result of Defendant's conduct. Defendant failed to institute adequate security measures that led to a data breach and allowed hackers to access the Private Information. Now that Plaintiffs' and Class Members' Private Information has been accessed and absconded with, it is available for criminal elements to sell or trade and will continue to be at risk for the indefinite future. In fact, the U.S. Government Accountability Office

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

found that, "bad actors can use stolen information for years after a breach."[49]

Medical Information

166. STIIIZY's security failures allowed cybercriminals to obtain medical information about Plaintiffs and the Class Members, including medical cannabis cards and any items purchased for medical use.

167. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[50]

168. Because medical information cannot be changed, this harm cannot be mitigated, and Plaintiffs and Class Members will bear the burden of having their medical information held by cybercriminals and sold.

169. Additionally, due to the social stigma and legal status of cannabis, the simple fact that someone purchased a product from STIIIZY or has a medical cannabis card is highly private information that Plaintiffs wish to keep confidential. For example, Plaintiff G.E. sought to proceed pseudonymously so as not to make his association with STIIIZY public.

170. The specific data compromised in this Data Breach – including social security numbers, medical cannabis cards, driver's licenses, and other information – is precisely the kind of information that can be used to perpetrate medical identity theft. According to the Federal Trade Commission, "[m]edical identity theft is when

---

[49] See *Data Breaches: Range of Consumer Risks Highlights Limitations of Identity Theft Services, U.S. GOV'T ACCOUNTABILITY OFF*. (2019), available at https://www.gao.gov/assets/700/698899.pdf.

[50] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

someone uses your personal information — like your name, Social Security number, health insurance account number or Medicare number — to get medical care, see a doctor, get prescription drugs, buy medical devices, or submit claims with your insurance provider."[51]

Social Security Numbers and Payment Information

171. Social Security numbers and payment information can also be used to commit fraud and identity theft. "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[52] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account."[53]

Driver's License Information

172. Driver's license numbers, which were compromised in the Data Breach, are incredibly valuable. "Hackers harvest license numbers because they're a very

---

[51] *Medical Identity Theft: What to Know, What to Do*, FEDERAL TRADE COMMISSION (2019), https://www.bulkorder.ftc.gov/system/files/publications/973a-medical-idtheft-what-to-know-what-to-do-508.pdf.

[52] *See* Husayn Kassai, *Banks need to stop relying on Social Security numbers*, AMERICAN BANKER (Nov. 12, 2018), https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers.

[53] *See What Can Someone Do With Your Social Security Number?*, CREDIT (Oct. 19, 2023), https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

valuable piece of information."[54]

173. A driver's license can be a critical part of a fraudulent, synthetic identity – which go for about $1,200 on the Dark Web. On its own, a forged license can sell for around $200."[55]

174. According to the national credit bureau Experian:

> A driver's license is an identity thief's paradise. With that one card, someone knows your birthdate, address, and even your height, eye color, and signature. If someone gets your driver's license number, it is also concerning because it's connected to your vehicle registration and insurance policies, as well as records on file with the Department of Motor Vehicles, place of employment (that keep a copy of your driver's license on file), doctor's office, government agencies, and other entities. Having access to that one number can provide an identity thief with several pieces of information they want to know about you. Next to your Social Security number, your driver's license number is one of the most important pieces of information to keep safe from thieves.

175. According to cybersecurity specialty publication CPO Magazine, "[t]o those unfamiliar with the world of fraud, driver's license numbers might seem like a relatively harmless piece of information to lose if it happens in isolation."[56] However, this is not the case. As cybersecurity experts point out:

> "It's a gold mine for hackers. With a driver's license number, bad actors can manufacture fake IDs, slotting in the number for any form that

---

[54] *Hackers Stole Customers' License Numbers From Geico In Months-Long Breach*, Forbes, Apr. 20, 2021, available at https://www.forbes.com/sites/leemathews/2021/04/20/hackers-stole-customers-license-numbers-from-geico-in-months-long-breach/?sh=3bda585e8658.

[55] *Id*.

[56] Scott Ikeda, *Geico Data Breach Leaks Driver's License Numbers, Advises Customers to Watch Out for Fraudulent Unemployment Claims*, CPO (Apr. 23, 2021), https://www.cpomagazine.com/cyber-security/geico-data-breach-leaks-drivers-license-numbers-advises-customers-to-watch-out-for-fraudulent-unemployment-claims/.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

requires ID verification, or use the information to craft curated social engineering phishing attacks."[57]

176. Plaintiffs and Class Members are now vulnerable to a full gamut of cybercrimes, loss in value of their property, and have been forced to take remedial action, as listed below.

Digital Phishing Scams

177. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $57 million to such scams in 2019 alone.[58]

178. Because a person's identity is akin to a puzzle with multiple data points, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity--or track the victim to attempt other hacking crimes against the individual to obtain more data to perfect a crime.

179. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate and trick individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails. Data Breaches can be the starting point for these additional targeted attacks on the victim.

---

[57] *Id.*

[58] *See How to Recognize and Avoid Phishing Scams*, FEDERAL TRADE COMMISSION CONSUMER ADVICE (2022), https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams.

180. Another such example of criminals piecing together bits and pieces of compromised Private Information for profit is the development of "Fullz" packages.[59]

181. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

182. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data (like phone numbers and emails) of Plaintiffs and the other Class Members.

183. Thus, even if certain information was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

184. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like phishing scammers).

---

[59] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

185. Defendant knew or should have known of the dangers of digital phishing scams. When Personal Information is employed in a social engineering scheme, criminals can gain unfettered access to individuals, or corporate databases, as the Data Breach itself evinces.

186. Defendant's customers are now more likely to become victims of digital phishing attacks because of the compromised information.

Loss of Time

187. As a result of this breach, Plaintiffs and impacted consumers will suffer unauthorized email solicitations, and experience a significant increase in suspicious phishing scam activity via email, phone calls, and text messages following the breach. In addition, the Plaintiffs, as a result of the breach, have spent significant time and effort researching the breach, monitoring their accounts for fraudulent activity, and dealing with increased unsolicited emails and texts.

Threat of Identity Theft

188. As a direct and proximate result of Defendant's breach of confidence, and failure to protect Private Information, Plaintiffs and the Class have also been injured by facing ongoing, imminent, impending threats of identity theft crimes, fraud, scams, and other misuse of this Private Information, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen Private Information, illegal sales of the compromised Private Information on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, lost work time, and other injuries. Defendant, through its misconduct, has enabled numerous bad actors to sell and profit off of Private Information that belongs to Plaintiffs.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Out of Pocket Costs

189. Plaintiffs are now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiffs anticipate spending out of pocket expenses to pay for these services.

Diminution in Value of a Valuable Property Right

190. Because personal data is valuable personal property, market exchanges now exist where internet users like Plaintiffs and Class Members can sell or monetize their own personal data.

191. 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 legitimate marketers or app developers.[60] For example, consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[61]

192. Moreover, Private Information derives its value from its confidential nature and consumers use it to verify identities, gain access to financial services, and verify eligibility for employment. Once the confidential nature of Private Information is destroyed, consumers ability to use that information unfettered is impacted and the value of that information is diminished.

193. Accordingly, as a result of the Data Breach, Plaintiffs lost the sale value of their Private Information and the opportunity to control how it is used. The fact that a threat actor specifically targeted Defendant demonstrates just how valuable

---

[60] *See*, *e.g.*, *The Personal Data Revolution*, DATACOUP, https://datacoup.com/.

[61] Nielsen Computer & Mobile Panel, *Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html.

Plaintiffs' Private Information can be to hackers and the significant value of Plaintiffs' Private Information to cybercriminals.

Loss of Privacy and Dignitary Harm

194. A data breach represents a significant violation of privacy, extending far beyond the mere loss of data. When sensitive personal information is compromised, individuals face a cascade of potential harm that erodes their sense of security and control, as information that they thought would remain confidential and private has now been leaked to the outside world, and which they no longer exercise control over. This exposure can lead to a profound sense of vulnerability, as individuals grapple with the knowledge that their most personal details are now in the hands of unknown actors, free to circulate and be publicized now, or at any time in the future.

195. Harm relating to an individual's loss of privacy and dignitary harm has also long been recognized by courts and in the common law. When an individual loses this privacy, such as here through its acquisition by criminal third parties, this harm cannot be undone. The Defendant's failure to safeguard this sensitive information has stripped Plaintiffs and the Class Members of this essential control, in addition to the economic damages they have incurred. This is especially damaging for Plaintiffs and Class Members since the information relates to their purchases of cannabis, which still carries a social stigma and is illegal under federal law.

196. This is a fundamental violation of an individual's control over their own personal narrative and image to which they provide the world. By stripping Plaintiffs and the Class Members of their right to control this information about themselves, Defendant has done immense harm to their rights to privacy as well as their personal dignity and sovereignty. As a result, while difficult to quantify, this harm is very real, long-lasting, and severe and has caused real damage to Plaintiffs and the Class

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Members, both emotionally as well as through their permanent loss of security and fundamental right to privacy.

Summary of Actual Economic and Noneconomic Damages

197. In sum, Plaintiffs and similarly situated consumers were injured as follows:

i. Theft of their Private Information and the resulting loss of privacy rights in that information;

ii. Improper disclosure of their Private Information;

iii. Loss of value of their Private Information;

iv. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

v. Defendant's retention of profits attributable to Plaintiffs' and other customers' Private Information that Defendant failed to adequately protect;

vi. Economic and non-economic impacts that flow from the imminent, and ongoing threat of fraud and identity theft to which Plaintiffs are now exposed;

vii. Ascertainable out-of-pocket expenses and the value of Plaintiffs' time allocated to fixing or mitigating the effects of this data breach;

viii. Overpayments for Defendant's products and/or services;

ix. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

F. Defendant Should Have Invested in Appropriate & Necessary Data Security

198. In the years immediately preceding the Data Breach, Defendant knew or should have known that its computer systems were a target for cybersecurity attacks.

199. The FBI, FTC, GAO, U.S. Secret Service, United States Cybersecurity and Infrastructure Security Agency, State Attorney General Offices and many other government and law enforcement agencies, and hundreds of private cybersecurity and threat intelligence firms, have issued warnings that put Defendant on notice, long before the Data Breach, that

(1) cybercriminals were targeting companies who store personal health information, such as Defendant;

(2) cybercriminals were ferociously aggressive in their pursuit of large collections of Private Information like that in possession of Defendant;

(3) cybercriminals were selling large volumes of Private Information and corporate information on Dark Web portals; and

(4) the threats were increasing.

200. Prior to the Data Breach, Defendant thus knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' Private Information could be accessed, exfiltrated and utilized by nefarious individuals as the result of a cyberattack.

201. Data security experts advise that "the vast majority of data breaches are preventable" if companies follow widely-available advice on data security practices, including "continually audit[ing] and reevaluat[ing]" their data security practices;

being aware of and working proactively to counter cybercriminals' evolving techniques and approaches; and training and re-training their employees.[62]

202. The vast majority of data breaches are not only foreseeable but preventable, a fact well-established by cybersecurity experts, who have long warned that companies must routinely audit and re-evaluate their security practices, stay ahead of evolving cybercriminal tactics, and rigorously train employees to maintain security vigilance. Despite these widely known and readily implementable measures, Defendant chose to save costs and failed to take action to prevent a foreseeable data breach.

203. It also ignored repeated warnings from the U.S. Department of Health and Human Services and cybersecurity industry experts that the healthcare industry – of entities that have any medical data – is a high value target for cybercriminals seeking access to PHI. Had Defendant properly prepared itself and its employees to comply with industry standards, this Data Breach would have been preventable.

CLASS ALLEGATIONS

204. Plaintiffs bring this action on their own behalf and on behalf of all other persons similarly situated. The Class which Plaintiffs seek to represent comprises:

Nationwide Class:

> All persons whose Private Information was accessed, compromised, or stolen in the Data Breach announced by Defendant on January 7, 2025 (the "Class").

California Subclass:

> All persons who were citizens of California when doing business with Defendant, whose Private Information was

[62] Nate Nead, *How To Prevent A Data Breach In Your Company*, FORBES (July 30, 2021), https://www.forbes.com/sites/forbesbusinesscouncil/2021/07/30/how-to-prevent-a-data-breach-in-your-company/?sh=3828f7b918da.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

> accessed, compromised, or stolen in the Data Breach announced by Defendant on January 7, 2025 (the "California Subclass").

This definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

205. The Class is comprised of hundreds of thousands of STIIIZY customers who have purchased items from STIIIZY in the past and were part of the Data Breach (the "Class Members"). The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

206. STIIIZY has claimed that "the incident only impacted consumer profiles associated with" four STIIIZY locations, all in California. Plaintiffs reserve the right to seek to expand the Class if it is found that the Data Breach involved STIIIZY locations in the other states that it operates.

207. There is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented in that the Class was exposed to the same common and uniform false and misleading advertising and omissions. The questions of law and fact common to the Class predominate over questions which may affect individual Class members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant's conduct is an unlawful business act or practice within the meaning of Business and Professions Code § 17200, *et seq*.;

b. Whether Defendant's conduct is an unfair business act or practice within the meaning of Business and Professions Code § 17200, *et seq*.;

c. Whether Defendant's conduct is a fraudulent business act or practice within the meaning of Business and Professions Code § 17200, *et seq*.;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

d. Whether Defendant's conduct is in violation of California Civil Code § 56, *et seq.*;

e. Whether Defendant's conduct is in violation of California Civil Code §§ 1709 and 1710;

f. Whether Defendant's failure to implement effective security measures to protect Plaintiffs' and the Class Members' Private Information was negligent;

g. Whether Defendant represented to Plaintiffs and the Class that it would protect Plaintiffs' and the Class Members' Private Information;

h. Whether Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

i. Whether Defendant breached a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

j. Whether Class Members' Private Information was accessed, compromised, or stolen in the Data Breach;

k. Whether Defendant's conduct caused or resulted in damages to Plaintiffs and the Class;

l. Whether Defendant failed to notify the public of the breach in a timely and adequate manner;

m. Whether Defendant knew or should have known that its systems, including but not limited to training protocols, technical security measures, and policies, left it vulnerable to the Data Breach;

n. Whether Defendant adequately addressed the vulnerabilities that allowed for the Data Breach; and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

o. Whether, as a result of Defendant's conduct, Plaintiffs and the Class are entitled to damages and relief.

208. The Plaintiffs' claims are typical of the claims of the proposed Class, as Plaintiffs and Class Members were harmed by Defendant's uniform unlawful conduct.

209. Plaintiffs will fairly and adequately represent and protect the interests of the proposed Class. Plaintiffs have retained competent and experienced counsel in class action litigation and other complex litigation.

210. Plaintiffs and the Class have suffered injury because of Defendant's false, deceptive, and misleading representations.

211. Plaintiffs would not have given their Private Information to Defendant but for the reasonable belief that Defendant would safeguard their data and Private Information.

212. The Class is identifiable and readily ascertainable. Notice can be provided to such purchasers using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

213. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually.

214. The litigation and resolution of the Class Members' claims are manageable. Individual litigation of the legal and factual issues raised by Defendant's conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

215. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for Defendant.

216. Absent a class action, Defendant will likely retain the benefits of its wrongdoing. Because of the small size of the individual Class Members' claims, few, if any, Class Members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, Class Members will continue to suffer losses and Defendant (and similarly situated companies) will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

COUNT ONE
VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.* (*On Behalf of the California Subclass*)

217. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

A. "Unfair" Prong

218. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, *et seq*., a challenged activity is "unfair" when "any injury it causes outweighs any benefits provided to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

219. Defendant's conduct as alleged herein does not confer any benefit to consumers. Mishandling this data shows blatant disregard for its customers' privacy and security.

220. Defendant's conduct as alleged herein causes injuries to consumers who do not receive goods or services consistent with their reasonable expectations. Specifically, Defendant's customers would not have reason to believe that simply doing business with Defendant would place their Private Information in the hands of cybercriminals.

221. In its data breach notices and communications with Plaintiffs and Class Members, Defendant committed "unfair" acts by failing to include—or knowingly omitting—information regarding the cybercriminal group Everest and the leaking of Private Information on the Dark Web.

222. Defendant's conduct as alleged herein causes injuries to its customers, who entrusted Defendant with their Private Information and whose Private Information was leaked as a result of Defendant's unlawful conduct.

223. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure entities that are trusted with it use appropriate security measures. These policies are reflected in law, including the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code § 1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

224. Defendant's customers cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

225. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

226. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

227. Defendant could have furthered its legitimate business interests in ways other than its unfair conduct.

228. Defendant's conduct threatens members by misleadingly advertising its purported "commitment" to protecting Private Information while exposing members' Private Information to hackers. Defendant's conduct also threatens other entities, large and small, who play by the rules. Defendant's conduct stifles competition, has a negative impact on the marketplace, and reduces consumer choice.

229. All of the conduct alleged herein occurs and continues to occur in Defendant's operations. Defendant's wrongful conduct is part of a pattern or generalized course of conduct repeated consistently.

230. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

231. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs and the Class Members relied on and made their purchase decision in part based on Defendant's representations regarding its security measures and trusted that Defendant would keep their Private Information safe and secure. Plaintiffs accordingly provided their Private Information to Defendant, reasonably believing and expecting that their Private Information would be safe and secure. Plaintiffs paid an unwarranted premium for the products they received. Specifically, Plaintiffs paid for goods from Defendant since Defendant represented that doing business with it would be secure and private, when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to the Data Breach.

232. Plaintiffs and the Class Members would not have given Defendant their Private Information had they known that their Private Information was vulnerable to

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

a data breach. Plaintiffs and Class Members seek an order mandating that Defendant implement adequate security practices to protect customers' Private Information. Additionally, Plaintiffs and Class Members seek an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

B. "Unlawful" Prong

233. California Business and Professions Code Section 17200, *et seq*., identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.,* 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

234. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates California Civil Code Section 1750, *et seq.*

235. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

236. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Customer Records Act, Cal. Civ. Code § 1798.81.5 (requiring reasonable data security measures) and § 1798.82 (requiring timely breach notification), the FTC Act, 15 U.S.C. § 45, California's Confidentiality of Medical Information Act, Cal. Civ. Code § 56, California's Consumer Privacy Act, Cal. Civ. Code § 1798.100, and California common law.

237. Defendant knew or should have known of its unlawful conduct.

238. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

239. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

240. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

241. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

242. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs paid an unwarranted premium for Defendant's products, believing that Defendant would protect their PII and PHI from breach. Plaintiffs would not have purchased the products, paying or overpaying for the products, if they had known that their purchase would put their Private Information at risk. Plaintiffs and the Class would not have given Defendant their Private Information, had they known that their Private Information was vulnerable to a data breach. Likewise, Plaintiffs and Class Members seek an order mandating that Defendant implement adequate security practices to protect members' Private Information. Additionally, Plaintiffs and the Class Members seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

C. Plaintiffs and the Class are entitled to equitable relief as no adequate remedy at law exists.

243. Defendant has not yet implemented adequate protections to prevent a future data breach, nor has it given adequate notice to all affected class members, and therefore, the equitable relief requested here would prevent ongoing and future harm;

244. Injunctive relief is also necessary to prevent the members of general public from being misled by Defendant's misrepresentations regarding privacy and security of information;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

245. The equitable relief under the UCL creates a straightforward cause of action for violations of law. Furthermore, damages for non-UCL claims require additional elements or pre-suit notice letters, which would potentially eliminate the possibility of providing damages to the entire class, while restitution would provide certainty and remedy for all affected victims.

246. In addition, discovery—which has not yet been provided and/or completed—may reveal that the claims providing legal remedies are inadequate. At this time, forcing an election of remedies at the initial pleadings stage, in the absence of completed discovery regarding class certification and merits, is premature and likely to lead to subsequent, potentially belated, and hotly contested motions to amend the pleadings to add equitable remedies based on a lengthy historical recount of discovery and analysis of voluminous exhibits, transcripts, discovery responses, document productions, etc., as well as related motions to seal confidential information contained therein.

COUNT TWO
CALIFORNIA CONSUMER PRIVACY ACT, CALIFORNIA CIVIL CODE § 1798.100, *et seq.*
(*On Behalf of the California Subclass*)

247. Plaintiffs, individually and on behalf of the California Subclass, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

248. Defendant boasts over 2 dozen locations in California alone as well as numerous cultivation, manufacturing, and distribution facilities throughout the state.[63]

249. Defendant STIIIZY also has significant revenue, with an estimated annual revenue between $100 Million to $1 Billion dollars, between 1,001-5,000

[63] *Assets*, STIIIZY, https://www.stiiizy.com/pages/assets.

employees, and having recently received financing of $36,000,000 as part of its operations.[64]

250. STIIIZY is considered a "business" as that term is defined in Cal. Civ. Code. § 1798.140(c) because, on information and belief, it has an annual gross revenue exceeding $25 million and it buys, receives, sells, or shares personal information of 50,000 or more consumers, households, or devices.

251. Plaintiffs' and California Subclass Members' PII is "nonencrypted and nonredacted personal information" consisting of social security number, names, addresses and other sensitive personal information. Cal. Civ. Code § 1798.150(a)(1). The Data Breach constitutes "an unauthorized access and exfiltration, theft, or disclosure" pursuant to Cal. Civ. Code § 1798.150(a)(1) because due to Defendant's failure to implement reasonable and necessary security measures, it enabled third party criminals to access personal information and thus, caused unauthorized sharing of Plaintiffs' and the California Subclass Members' personal information.

252. Defendant had a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of Plaintiffs' and California Subclass Members' PII to protect said PII.

253. Defendant breached the duty they owed to Plaintiffs and California Subclass Members described above. Defendant breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the PII of Plaintiffs and California Subclass Members; (b) detect the breach while it was ongoing; and (c) maintain security systems consistent with industry standards.

---

[64] *STIIIZY Company Overview*, LEADIQ, https://leadiq.com/c/stiiizy/5d16634d1f0000ff0027160a.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

254. Defendant's breach of the duty they owed to Plaintiffs and the California Subclass Members described above was the direct and proximate cause of the Data Breach. As a result, Plaintiffs and the California Subclass Members suffered damages, as described above and as will be proven at trial.

255. Plaintiffs and the California Subclass Members seek injunctive relief in the form of an order enjoining Defendant from continuing the practices that constituted their breach of the duty owed to the Plaintiffs and California Subclass Members as described above, together with actual and statutory damages.

COUNT THREE
VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT
Cal. Civ. Code §§ 1750 *et seq*.
(*On Behalf of the California Subclass*)

256. Plaintiffs, individually and on behalf of the California Subclass, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

257. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "CLRA"), California Civil Code § 1750, *et seq*.

258. Plaintiffs and California Subclass Members are "consumers," as the term is defined by California Civil Code § 1761(d) because they purchased products for personal, family, or household purposes from Defendant.

259. Plaintiffs, California Subclass Members, and Defendant have engaged in "transactions," as that term is defined by California Civil Code § 1761(e), since Plaintiffs, California Subclass Members, and Defendant entered into agreements and performed those agreements when they made purchases of goods from Defendant in exchange for payment.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

260. The conduct alleged in this Complaint constitutes unfair methods of competition and unfair and deceptive acts and practices for the purpose of the CLRA, and the conduct undertaken by Defendant was likely to deceive consumers.

261. Cal. Civ. Code § 1770(a)(5) prohibits one who is involved in a transaction from "[r]epresenting that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities which they do not have."

262. Defendant violated this provision by representing that Defendant took appropriate measures to protect Plaintiffs' and the California Subclass Members' Private Information.

263. As a result, Plaintiffs and the California Subclass Members were induced to provide their Private Information to Defendant.

264. As a result of engaging in such conduct, Defendant has violated Civil Code § 1770.

265. Pursuant to California Civil Code section 1782, on March 20, 2025, Plaintiffs' counsel, acting on behalf of Plaintiff G.E. and members of the Class, mailed a Demand Letter, via U.S. certified mail, return receipt requested, addressed to Defendant at its headquarters and principal place of business, and to its registered agent for service of process, which was delivered on March 27, 2025.

266. Plaintiffs also seek damages from Defendant for violation of the CLRA in the form of damages, disgorgement, or ill-gotten gains to compensate Plaintiff and the California Subclass.

267. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiffs seek an order of this Court that includes, but is not limited to, an order enjoining Defendant from continuing to engage in unlawful, unfair, or fraudulent business practices or any other act prohibited by law.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

268. Plaintiffs and the California Subclass Members suffered injuries caused by Defendant's misrepresentations, because they provided their Private Information believing that Defendant would adequately protect this information.

269. Plaintiffs and California Subclass Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

270. The unfair and deceptive acts and practices of Defendant, as described above, present a serious threat to Plaintiffs and the California Subclass Members.

COUNT FOUR
VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT
Cal. Civ. Code § 1798.80, *et seq*.
(*On Behalf of the California Subclass*)

271. Plaintiffs, individually and on behalf of the California Subclass, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

272. To ensure that personal information about California residents is protected, the California Legislature enacted the Customer Records Act ("CRA"), California Civil Code § 1798.81.5, which requires that any business that "owns licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

273. As described above, Defendant failed to implement and maintain reasonable security procedures and practices to protect the Plaintiffs' and California Subclass Members' Private Information, and thereby violated the California CRA.

274. Under California Civil Code § 1798.82, any business that obtains and retains Private Information must promptly and "in the most expedient time possible and without unreasonable delay" disclose any Data Breach involving such retained data.

275. Any customer injured by a violation of California Civil Code § 1798.82 "may institute a civil action to recover damages." Cal. Civ. Code § 1798.84(b).

276. By its above-described wrongful actions, inaction, omissions, and want of ordinary care, Defendant failed to design, adopt, implement, control, direct, oversee, manage, monitor and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect the Plaintiffs' and California Subclass Members' Private Information.

277. Defendant also unreasonably delayed and failed to disclose the Data Breach (and threat of the data breach) to the Plaintiffs and California Subclass Members in the most expedient time possible and without unreasonable delay when they knew, or reasonably believed, the Plaintiffs and California Subclass Members' Private Information had been wrongfully disclosed to an unauthorized person or persons.

278. As a direct and proximate result of Defendant's above-described wrongful actions, inaction, omissions, and want of ordinary care that directly and proximately caused the Data Breach and its violations of the California CRA, the Plaintiffs and California Subclass Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, *inter alia*, (i) an imminent, immediate and continuing increased risk of identity theft and identity fraud – risks justifying expenditures for protective and remedial services for which they are entitled to compensation, (ii) invasion of privacy, (iii) breach of the confidentiality of their Private Information, (iv) statutory damages, (v) deprivation of the value of their Private Information, for which there is a well-established national and international market, and/or (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

279. Accordingly, the Plaintiffs and the California Subclass Members are entitled to actual damages under California Civil Code § 1798.84(b).

280. The Plaintiffs and California Subclass Members are also entitled to injunctive relief under California Civil Code § 1798.84(e).

COUNT FIVE
VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION ACT
Cal. Civ. Code § 56, *et seq.*
(*On Behalf of the Nationwide Class*)

281. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

282. Defendant is subject to the requirements and mandates of the Confidentiality of Medical Information Act ("CMIA") because it is a "contractor" and/or "provider of health care" pursuant to Cal. Civ. Code § 56.06.

283. CMIA § 56.36 allows an individual to bring an action against a "person or entity who has negligently released confidential information or records concerning him or her in violation of this part."

284. As a direct result of its negligent failure to adequately protect the data it collected from the Plaintiffs and Class Members, in violation of Cal. Civ. Code § 56.101, Defendant allowed for a Data Breach which released the Private Information of Plaintiffs and Class Members to criminals and/or third parties.

285. The CMIA defines "medical information" as "any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care . . . regarding a patient's medical history, mental or physical condition, or treatment."

286. The CMIA defines individually identifiable information as "medical information [that] includes or contains any element of personal identifying

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

information sufficient to allow identification of the individual, such as the [customers]' name, address, electronic mail address, telephone number, or social security number, or other information that, alone or in combination with other publicly available information, reveals the individual's identity." Cal. Civ. Code § 56.050.

287. Defendant is in possession of affected individuals' medical information, as it has indicated that its customers' medical cannabis cards were lost in the data breach. Thus, information relating to the diagnosis and treatment of patients/customers, at minimum, was exposed in the data breach. Further, the compromised data was individually identifiable because it was accompanied by elements sufficient to allow identification of Plaintiffs by the third parties to whom the data was disclosed. Class Members' names, photographs, and addresses were included in the compromised data.

288. Defendant came into possession of Plaintiffs' and Class Members' medical information and had a duty pursuant to Section 56.06 and 56.101 of the CMIA to maintain, store and dispose of the Plaintiffs' and Class Members' medical records in a manner that preserved their confidentiality. Sections 56.06 and 56.101 of the CMIA prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential medical information.

289. Defendant further violated the CMIA by failing to use reasonable care, and in fact, negligently maintained Plaintiffs' and Class Members' medical information, allowing and enabling a threat actor to view and access unencrypted PHI for Class Members.

290. Since Defendant directed the usage, storage, and other actions and/or inactions concerning Plaintiffs' and Class Members' medical information in California, the CMIA equally applies to the entire affected Class. *See, e.g., Doe v.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Meta Platforms, Inc., No. 22-cv-03580-WHO, 2023 U.S. Dist. LEXIS 158683, at *16 (N.D. Cal. Sep. 7, 2023) (holding that another statute, CIPA, could apply to non-residents of California, because the conduct at issue occurred in California).

291. As a direct and proximate result of Defendant's violations of the CMIA, Plaintiffs and Class Members have been injured and are entitled to compensatory damages, punitive damages, and nominal damages of one-thousand dollars ($1,000) for each of Defendant's violations of the CMIA, as well as attorneys' fees and costs pursuant to Cal. Civ. Code § 56.36.

COUNT SIX
NEGLIGENCE
(*On Behalf of the Nationwide Class*)

292. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

293. Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their Private Information. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that consumers' Private Information was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

294. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiffs and Class Members, who were the foreseeable and probable victims of any inadequate security practices. 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 entities such as

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Defendant for failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

295. Defendant violated Section 5 of the FTC Act, Customer Records Act, California Civil Code § 1798.81.5, and the Confidentiality of Medical Information Act, Cal. Civ. Code § 56 *et seq*. by failing to use reasonable measures to protect Plaintiffs' and Class Members' Private Information and not complying with the industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored and the foreseeable consequences of a data breach involving Private Information of Plaintiffs and the Class Members.

296. Plaintiffs and the Class Members are within the Class of persons these statutes and regulations were intended to protect. The harms which occurred, including the loss of privacy, significant risk of identity theft, and overpayment for goods and services, are the types of harm that these statutes and their regulations were intended to prevent.

297. Defendant also had a special relationship with Plaintiffs and Class Members, which is recognized by laws and regulations, as well as common law. Defendant was in a position to ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach. Plaintiffs and Class Members were compelled to entrust Defendant with their Private Information. At all relevant times, Plaintiffs and Class Members understood that Defendant would take adequate security precautions to safeguard that information. Only Defendant had the ability to protect Plaintiffs' and Class Members' Private Information that it held.

298. Defendant knew or should have known that Plaintiffs' and the Class Members' Private Information is information that is frequently sought after by criminals.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

299. Defendant knew or should have known that Plaintiffs and the Class Members would suffer harm if their Private Information was leaked.

300. Defendant knew or should have known that its security systems were not adequate to protect Plaintiffs' and the Class Members' Private Information from a data breach.

301. Defendant knew or should have known that adequate and prompt notice of the Data Breach was required such that Plaintiffs and the Class Members could have taken more swift and effective action to change or otherwise protect their Private Information. Defendant failed to provide timely notice upon discovery of the data breach. Class Members were informed of the data breach on January 7, 2025, with many not receiving actual notice. Defendant had learned of the data breach nearly two months prior, in November 2024.

302. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and the Class Members' Private Information by failing to design, implement, and maintain adequate security measures to protect this information. Moreover, Defendant did not implement, design, or maintain adequate measures to detect a data breach when it occurred.

303. Defendant's conduct as described above constituted an unlawful breach of its duty to provide adequate and prompt notice of the data breach.

304. Plaintiffs' and the Class Members' Private Information would have remained private and secure had it not been for Defendant's wrongful and negligent breach of its duties. The leak of Plaintiffs' and the Class Members' Private Information, and all subsequent damages, was a direct and proximate result of Defendant's negligence.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

305. Defendant's negligence was, at least, a substantial factor in causing Plaintiffs' and the Class Members' Private Information to be improperly accessed, disclosed, and otherwise compromised, and in causing Class Members' other injuries arising out of the Data Breach.

306. The damages suffered by Plaintiffs and the Class were the direct and reasonably foreseeable result of Defendant's negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiffs' and Class Members' Private Information.

307. Defendant knew or should have known that its security for safeguarding Plaintiffs' and Class Members' Private Information was inadequate and vulnerable to a data breach.

308. Defendant's negligence directly caused significant harm to Plaintiffs and Members of the Class.

COUNT SEVEN
INVASION OF PRIVACY
(*On Behalf of the Nationwide Class*)

309. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

310. Plaintiffs and Class Members had a reasonable and legitimate expectation of privacy in their Private Information that Defendant failed to adequately protect against compromise from unauthorized third parties.

311. Defendant owed a duty to Plaintiffs and Class Members to keep their Private Information confidential.

312. Defendant failed to protect, and released to unknown and unauthorized third parties, the Private Information of Plaintiffs and Class Members.

313. By failing to keep Plaintiffs' and Class Members' Private Information safe, knowingly utilizing unsecure systems and practices, Defendant unlawfully

invaded Plaintiffs' and Class Members' privacy by, among others, (i) intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; (ii) failing to adequately secure their Private Information from disclosure to unauthorized persons and/or third parties; and (iii) enabling the disclosure of Plaintiffs' and Class Members' Private Information without consent.

314. Defendant knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

315. Defendant knew, or acted with reckless disregard of the fact that, organizations handling PII or PHI are highly vulnerable to cyberattacks and that employing inadequate security and training practices would render them especially vulnerable to data breaches.

316. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Private Information were unduly frustrated and thwarted, thereby causing Plaintiffs and the Class Members undue harm.

317. Plaintiffs seek injunctive relief on behalf of the Class, restitution, as well as any and all other relief that may be available at law or equity. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause irreparable injury to Plaintiffs and Class Members. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

COUNT EIGHT
BREACH OF IMPLIED CONTRACT
(*On Behalf of the Nationwide Class*)

318. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

319. At all relevant times, Defendant had a duty, or undertook and/or assumed a duty, to implement a reasonable data privacy and cybersecurity protocol, including adequate prevention, detection, and notification procedures, in order to safeguard the Private Information of Plaintiffs and the Class Members, and to prevent the unauthorized access to and disclosures of this data.

320. Among other things, Plaintiffs and Class Members were required to disclose their Private Information to Defendant when doing business with it, as well as implied contracts for the Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

321. When Plaintiffs and Class Members provided their Private Information to Defendant, they entered into implied contracts with Defendant pursuant to which Defendant agreed to reasonably protect such information.

322. By entering into such implied contracts, Plaintiffs and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations and were consistent with industry standards.

323. Under implied contracts, Defendant and/or their affiliated providers promised and were obligated to protect Plaintiffs' and Class Members' Private Information. In exchange, Plaintiffs and Members of the Class agreed to turn over their Private Information.

324. The implied contracts that include the contractual obligations to maintain the privacy of Plaintiffs' and Class Members' Private Information, are also

acknowledged, memorialized, and embodied in multiple documents, including (among other documents) Defendant's Data Breach notification and Defendant's Privacy Policy.

325. Defendant's express representations, including, but not limited to the express representations found in their notices of privacy practices, memorialize and embody the implied contractual obligations requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

326. Plaintiffs and Class Members performed their obligations under the contract when they provided their Private Information in consideration for Defendant's goods and/or services.

327. Defendant materially breached its contractual obligations to protect the Private Information it gathered when the information was accessed and exfiltrated during the Data Breach.

328. Defendant materially breached the terms of the implied contracts, including, but not limited to, the terms stated in the relevant notices of privacy practices. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by their notification of the Data Breach to Plaintiffs and Class Members.

329. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

330. As a result of Defendant's failure to fulfill the data security protections promised in these contracts, Plaintiffs and Class Members did not receive full benefit of the bargain they entered into.

331. Had Defendant disclosed that their security was inadequate or that they did not adhere to industry-standard security measures, neither Plaintiffs, Class

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Members, nor any reasonable person would have entered into the aforementioned agreements with Defendant.

332. As a direct and proximate result of the data breach, Plaintiffs and Class Members have been harmed and suffered, and will continue to suffer, actual damages and injuries, including without limitation the release and disclosure of their Private Information, the loss of control of their Private Information, the imminent risk of suffering additional damages in the future, out of pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

COUNT NINE
UNJUST ENRICHMENT
(*On Behalf of the Nationwide Class*)

333. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

334. Defendant funds its data security measures entirely from their general revenues, including payments made by or on behalf of Plaintiffs and Class Members.

335. A portion of the payments made by or on behalf of Plaintiffs and Class Members was to be used to provide the necessary level of data security.

336. Plaintiffs and the Class conferred a monetary benefit on Defendant by purchasing the products from Defendant and in doing so provided Defendant with their most sensitive PII and PHI. In exchange, Plaintiffs and Class Members should have received from Defendant the products that were subject to the transaction and had their PII protected with adequate data security measures.

337. Defendant knew that Plaintiffs and the Class conferred a benefit which it accepted, and through which Defendant was unjustly enriched. Defendant profited from these transactions and used Plaintiffs' and the Class Members' Private Information for business purposes to increase their revenues.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

338. Defendant enriched itself by saving the costs it reasonably should have spent on the necessary data security measures to secure Plaintiffs' and the Class Members' Private Information. Instead of providing the necessary level of security that would have prevented the Data Breach, Defendant instead calculated to increase their own profits at the expense of Plaintiffs and the Class, by using ineffective security measures, failing to pay money for the much-needed training of their employees, failing to conduct the audits, and implementing other security measures discussed above. Plaintiffs and the Class suffered an injury as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security and training.

339. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiffs and the Class, because it failed to implement appropriate data management and security measures as mandated by common law and statutory duties.

340. If Plaintiffs and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide this information nor would they have done business with Defendant.

341. Plaintiffs and the Class have no adequate remedy at law as discussed above.

342. Defendant should be compelled to disgorge its profits and/or proceeds that it unjustly received as a result of having Plaintiffs' and Class Members' Private Information, or alternatively, Defendant should be compelled to refund the amounts that Plaintiffs and the Class overpaid for its goods.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

COUNT TEN
DECLARATORY JUDGMENT AND INJUNCTIVE RELIEF
(*On Behalf of the Nationwide Class*)

343. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

344. The Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq*., authorizes this Court to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief.

345. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

346. Defendant owes a duty of care to Plaintiffs and Class Members which require it to adequately secure its Private Information when it chose to accept and store Plaintiffs' and Class Members' Private Information.

347. Defendant still possesses Plaintiffs' and Class Members' Private Information.

348. Defendant does not specify in the Data Breach notification posted on its website what specific and verifiable steps it has taken to prevent a similar breach from occurring again.

349. Plaintiffs and Class Members are at risk of harm due to the exposure of their Private Information and the Defendant's failures to address the security failings that led to such exposure.

350. An actual controversy has arisen in the wake of the Data Breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard Plaintiffs' and Class Members' Private Information and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Class from further data breaches that compromise their Private Information.

351. Plaintiffs and the Class, therefore, seek a declaration that (1) each of Defendant's existing security measures do not comply with its obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect consumers' Private Information, and (2) to comply with its duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide notice to all affected consumers);

b. Requiring Defendant to implement adequate security protocols and practices to protect consumers' Private Information consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

c. Mandating the proper notice be sent to all affected consumers, and posted publicly;

d. Requiring Defendant to protect all data collected through any account creation requirements;

e. Requiring Defendant to delete, destroy, and purge the Private Information of Plaintiffs and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' Private Information;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

g. Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h. Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

i. Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

j. Requiring Defendant to conduct systematic scanning for data breach related issues;

k. Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the Private Information data; and

l. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

352. The Court can, and should, issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with the law and industry standards to protect Plaintiffs' and Class Members' Private Information.

353. If an injunction is not issued, Plaintiffs and the Class will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

breach of the Defendant's systems or networks. The risk of another breach is real, immediate, and substantial.

354. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. If another data breach occurs, the Plaintiffs and the Class will likely be subjected to fraud, identity theft, and other harms described herein. However, the cost to the Defendant of complying with an injunction by employing reasonable prospective data security measures is minimal given they have preexisting legal obligations to employ these measures.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, request judgment and relief on all causes of action as follows:

A. That the Court determine that this Action may be maintained as a Class Action, that Plaintiffs be named as Class Representatives, that the undersigned be named as Class Counsel for the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order declaring that Defendant's actions, as set forth in this Complaint, violate the laws set forth above;

C. That the Court enter an order providing declaratory and injunctive relief including specific steps, as outlined above, requiring Defendant to utilize appropriate methods and policies as necessary to remediate the harm suffered by Plaintiffs and the Class members as well as to prevent future harm and properly secure its data;

D. That the Court award Plaintiffs and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiffs and the Class are entitled, including, but not limited to, restitution and an Order requiring Defendant to cooperate and financially support recovery efforts;

F. That the Court award Plaintiffs and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

G. That the Court award Plaintiffs and the Class their reasonable attorneys' fees and costs of suit;

H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and

I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs respectfully demand a trial by jury for all claims.

Respectfully submitted,

CLARKSON LAW FIRM, P.C.

/s/ Yana Hart
CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson, Esq. (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart, Esq. (SBN 306499)
yhart@clarksonlawfirm.com
Bryan P. Thompson, Esq. (SBN 354683)
bthompson@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050

COTCHETT PITRE & MCCARTHY, LLP
Thomas E. Loeser, Esq. (SBN 202724)
tloeser@cpmlegal.com
2716 Ocean Park Blvd., Ste. 3088
Santa Monica, CA 90405
Tel: (206) 802-1272
Fax: (310) 392-0111

Karin B. Swope (*pro hac vice* forthcoming)
kswope@cpmlegal.com
Ellen J Wen (*pro hac vice* forthcoming)
ewen@cpmlegal.com
1809 7th Avenue, Suite 1610
Seattle, WA 98101
Tel: (206) 802-1272
Fax: (205) 299-4184

Interim Co-Lead Counsel for Plaintiffs

CLAPP & LAUINGER LLP
James F. Clapp, Esq. (SBN 145814)
jclapp@clapplegal.com
701 Palomar Airport Road, Suite 300
Carlsbad, CA 92011
Tel: (760) 209-6565 ext. 101
Fax: (760) 209-6565

WYNNE LAW FIRM
Edward J. Wynne, Esq. (SNB 165819)
ewynne@wynnelawfirm.com
80 E. Sir Francis Drake Blvd., Ste. 3-G
Larkspur, CA 94939
Tel: (415) 461-6400
Fax: (415) 461-3900

CLAYEO C. ARNOLD
A PROFESSIONAL CORPORATION
M. Anderson Berry (SBN 262879)
aberry@justice4you.com
Gregory Haroutunian (SBN 330263)
gharoutunian@justice4you.com
Brandon P. Jack (SBN 325584)
bjack@justice4you.com
865 Howe Avenue
Sacramento, CA 95825
Tel: (916) 239-4778
Fax: (916) 924-1829

TOUSLEY BRAIN STEPHENS PLLC
Kaleigh N. Boyd (pro hac vice forthcoming)
kboyd@tousely.com
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600

AHDOOT & WOLFSON, PC
Tina Wolfson (SBN 174806)
twolfson@ahdootwolfson.com
Deborah De Villa (SBN 312564)
ddevilla@ahdootwolfson.com
2600 West Olive Avenue, Suite 500
Burbank, CA 91505
Tel: (310) 474-9111
Fax: (310) 474-8585

AHDOOT & WOLFSON, PC
Andrew W. Ferich *(pro hac vice* to be filed)
aferich@ahdootwolfson.com
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Tel: (310) 474-9111
Fax: (310) 474-8585

HEENAN & COOK
John Heenan (*Pro Hac Vice to be filed*)
john@lawmontana.com
1631 Zimmerman Trail
Billings, MT 59102
Tel: (406) 839-9091

STRAUSS BORRELLI PLLC
Andrew G. Gunem (SBN 354042)
agunem@straussborrelli.com
Raina C. Borrelli (*pro hac vice* forthcoming)
raina@straussborrelli.com
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Tel: (872) 263-1100
Fax: (872) 263-1109

SIGNATURE ATTESTATION

Pursuant to Local Rule 5-4.3.4(a)(2)(i), I hereby certify that all signatories concur with the content of this document and that I obtained authorization from them to affix their electronic signatures to this document.

Dated: July 3, 2025

/s/ Yana Hart
Yana Hart

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265