IN THE UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

MICAHEL WARSHAWSKY and MICHAEL STEINHAUSER, behalf of themselves and all others similarly situated, Plaintiffs, v. CDBMD, INC. and CBD INDUSTRIES, LLC, Defendants.	Case No.: _____ JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiffs Michael Warshawsky and Michael Steinhauser ("Plaintiffs") bring this Class Action Complaint against cbdMD, Inc. and CBD Industries, LLC (collectively, "CBD" or "Defendants") as individuals and on behalf of all others similarly situated, and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. CBD manufacture and distribute hemp products, including cannabidiol oils for pain relief and sleep aid. CBD sells their products to consumers throughout the nation via their website, cbdMD.com. Founded in 2015, cbdMD, Inc. is publicly traded on the NYSE and claims to have over 100 employees and an estimated annual revenue of over $25 million.

2. Beginning on or about September 25, 2020, CBD notified the U.S. Securities and Exchange Commission ("SEC"), various states' Attorneys' General, and thousands of affected customers about two data breaches that occurred through the cbdMD.com website from March 30, 2020 through May 8, 2020, and again from May 14, 2020 through May 18, 2020 (the "Data Breaches"). Hackers not only "scraped" many of CBD's consumers' names from Defendants'

website by infecting the ecommerce platform with a "malicious code," hackers also stole customers' payment card numbers, CVV security codes, credit card expiration dates, addresses, email addresses, and bank account numbers ("PII"). The criminals obtained everything they needed to illegally use CBD's customers' payment cards to make fraudulent purchases, and to commit myriad financial crimes and fraud.

3. Not only did hackers skim CBD's customers' PII, on information and belief, the stolen names and payment card information are now for sale on the dark web—a key motivating element for hackers engaged in data breaches of this type. Hackers accessed and then offered for sale the unencrypted, unredacted, stolen PII to criminals. Because of Defendants' Data Breaches, CBD consumers' PII is still available on the dark web for criminals to access and abuse. CBD's customers face a substantially increased risk of financial fraud.

4. All of this personally identifiable information was compromised due to Defendants' negligent and/or careless acts and omissions and the failure to protect customers' data. In addition to CBD's failure to prevent the Data Breaches, Defendants failed to detect the breaches for almost six months, and when they did discover the breaches Defendants informed their shareholders days before they informed the affected consumers, depriving their customers of precious time to put a stop to financial fraud as soon as possible. Indeed, the Data Breaches impacted CBD twice, demonstrating a repeated ability to penetrate CBD's networks and steal customers' PII.

5. The stolen PII has great value to hackers: thousands of CBD consumers—residents of many states—were affected by the Data Breaches. For example, CBD has filed data breach notices in California, Maine, New Hampshire, and Vermont, among others.[1]

[1] *See, e.g.*, CBD's *Notice of Data Privacy Incident to the New Hampshire Attorney General*, archived by the New Hampshire Attorney General on September 29, 2020, *available at*: https://www.doj.nh.gov/consumer/security-breaches/documents/cbd-industries-20200929.pdf (last accessed Oct. 8, 2020); CBD's *Notice of Data Breach*, archived by the California Attorney General on September 29, 2020, *available at*: https://oag.ca.gov/system/files/CA%20Notice%20%28B%26W%29.pdf (last accessed Oct. 8, 2020).

6. Plaintiff brings this action on behalf of all persons whose PII was compromised as a result of Defendants' failure to: (i) adequately protect their consumers' PII; (ii) warn consumers of their inadequate information security practices; and (iii) effectively monitor Defendants' websites and ecommerce platforms for security vulnerabilities and incidents. Defendants' conduct amounts to negligence and violates federal and state statutes.

7. Plaintiffs and similarly situated CBD customers ("Class members") have suffered injury as a result of Defendants' conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from financial fraud and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breaches, including but not limited to lost time; (iv) deprivation of rights they possess under Florida's Deceptive and Unfair Trade Practices Act (Florida Statute § 501.203, *et seq.*); (v) deprivation of rights they possess under the California Consumer Privacy Act, (Cal. Civ. Code § 1798.100, *et seq*. (§ 1798.150(a)); and (vi) the continued and certainly an increased risk to their PII, which: (a) remains available on the dark web for individuals to access and abuse; and (b) remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII.

PARTIES

8. Plaintiff Michael Warshawsky is a citizen of Florida residing in Debary, Florida. Mr. Warshawsky purchased CBD products from cdbMD.com on April 27, 2020, using his debit card. He received CBD's *Notice of Data Breach* on or about September 28, 2020.

9. Plaintiff Michael Steinhauser is a citizen of California residing in Granada Hills, California. Mr. Steinhauser purchased CBD products for his pet from cdbMD.com on April 25, 2020, using his debit card. He received CBD's *Notice of Data Breach* on or about September 28, 2020.

10. Defendant cbdMD, Inc., is a publicly traded, North Carolina corporation, with its principle place of business located at 8845 Red Oak Boulevard, Charlotte, North Carolina.

Defendants advertise and sell CBD-related products to residents nationwide through the website cbdMD.com.

11. Defendant CBD Industries, LLC, is a wholly owned manufacturing and distribution subsidiary of cbdMD, Inc., with its principle place of business also located at 8845 Red Oak Boulevard, Charlotte, North Carolina. According to the North Carolina Secretary of State,[2] the sole member of CBD Industries, LLC, is cbdMD, Inc., and therefore this limited liability company is a North Carolina citizen for purposes of jurisdiction.

12. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

13. All of Plaintiffs' claims stated herein are asserted against Defendants and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount in controversy exceeds the sum or value of $5,000,000, exclusive of interest and costs, there are more than 100 members in the proposed class. Moreover, this Court has jurisdiction over this action under 28 U.S.C. § 1332(a)(1) because Plaintiff Warshawsky is a Florida citizen, and Plaintiff Steinhauser is a California citizen, and therefore diverse from Defendants, which are North Carolina citizens.

15. This Court has personal jurisdiction over Defendants because Defendants are located in North Carolina, with their principal place of business within this District.

16. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from this District. Defendants reside within this judicial district and substantial part of

[2] North Carolina Secretary of State, *Business Search, available at:* https://www.sosnc.gov/online_ services/search/

the events giving rise to the claims alleged herein occurred within this judicial district.

FACTUAL ALLEGATIONS

Background

17. CBD manufactures hemp products, including hemp-based "bath bombs," clothing and cannabidiol oils and other products used for pain relief and general health for both humans and animals.[3] CBD sells their products to consumers throughout the nation via their website, cbdMD.com. The company's revenue rose during the summer of 2020 as a result of "a significant shift in online sales as an overall percentage of net sales, with direct to consumer e-commerce online sales reporting 72% of overall sales, up from 67% from the prior quarter."[4] The parent company, cbdMD, Inc. is publicly traded on the NYSE and claims to have estimated annual revenue of over $25 million.

18. Customers purchasing products online demand security to safeguard their PII. CBD claims that it "respects the privacy of [their consumers'] information," and touts in their Privacy Policy that it will only "disclose" their consumers' PII under certain circumstances: "To fulfill the purpose for which you provide it," and "To comply with any court order, law, or legal process, including to respond to any government or regulatory request." CBD states that it may also disclose their customers' "personal information to a third party for a business purpose [. . . .] When we disclose personal information for a business purpose, we enter a contract that describes the purpose and requires the recipient to both keep that personal information confidential and not use it for any purpose except performing the contract."

19. CBD does not state whether it is compliant with the Payment Card Industry Data

[3] The 2018 Farm Bill made it legal to produce, sell, and consume hemp and hemp-derived products throughout the United States. *See* https://www.agriculture.senate.gov/2018-farm-bill (last accessed Oct. 8, 2020). These products must be derived from industrial hemp containing less than 0.3 percent Tetrahydrocannabinol ("THC"). THC is a natural compo und found in cannabis plants – including hemp, but to a lesser degree compared with marijuana.

[4] *Right Now, cbdMD Stock Is a Speculation That Could Pay off Big*, Investorplace, June 22, 2020, *available at*: https://investorplace.com/2020/06/ycbd-stock-speculation-pay-off/ (last accessed Oct. 8, 2020).

Security Standard ("PCI DSS"), which is a requirement for businesses that store, process, or transmit payment card data. The PCI DSS defines measures for ensuring data protection and consistent security processes and procedures around online financial transactions.

20. As formulated by the PCI Security Standards Council, the mandates of PCI DSS compliance include, in part: Developing and maintaining a security policy that covers all aspects of the business, installing firewalls to protect data, and encrypting cardholder data that is transmitted over public networks using anti-virus software and updating it regularly.[5]

21. To purchase products on CBD's website, customers can create an account or check out as a guest. To complete a purchase, at a minimum, the customer must enter the following PII:

- Name;
- billing address;
- delivery address;
- email address;
- telephone number;
- name on the payment card;
- type of payment card;
- full payment card number;
- payment card expiration date; and
- security code, or CVV code (card verification number).

22. At no time during the final checkout process does CBD require customers to expressly agree to or review Defendants' "Privacy Policy" or "Terms & Conditions."

The Data Breaches

23. On or about September 25, 2020, before reporting the Data Breaches to their affected customers, cbdMD, Inc. filed a Form 8-K with the SEC, stating: "[CDB] recently determined the eCommerce platform underlying their online retail sales webpage, cbdmd.com, was modified by an unauthorized third-party to include malicious code."[6]

[5] PCI Security Standards Council, *available at*: https://www.pcisecuritystandards.org/ (last accessed Oct. 8, 2020).
[6] cbdMD, Inc.'s SEC Edgar Filing, Sept. 25, 2020, *available at*: http://filings.irdirect.net/data/1644903/000165495420010485/ycbd_8k.pdf (last accessed Oct. 8, 2020).

24. Beginning on or about September 29, 2020, almost six months after the Data Breaches started, CBD Industries, LLC sent a *Notice of Data Privacy Incident* to various states' Attorneys General. This Notice reiterated the information stated by its parent company in the Form 8-K, but added some details, including that the Data Breaches occurred "from March 30, 2020, through May 8, 2020, and May 14, 2020, through May 18, 2020." CBD's counsel admitted in the *Notice* that the "data elements at risk included both personal and non-personal information consisting of first and last names, email addresses, billing addresses, credit or debit card numbers, expiration dates and card security codes, and/or bank account numbers."

25. Beginning on or about September 28, 2020, CBD Industries, LLC sent its affected consumers a *Notice of Data Breach*, reiterating the information in the Form 8-K and the *Notice* to the Attorneys General. CBD added a section entitled "What We Are Doing." Defendants only response to the Data Breaches was to offer their affected consumers 12 months of "identity monitoring." Defendants did not admit to improving or securing their ecommerce platform, nor did they provide any details of their investigation into the Data Breaches.

26. CBD's consumers' information is likely for sale on the dark web and, on information and belief, is still for sale to criminals. This means that the Data Breaches were successful; unauthorized individuals accessed CBD's customers' unencrypted, unredacted information, including "first and last names, email addresses, billing addresses, credit or debit card numbers, expiration dates and card security codes, and/or bank account numbers," and possibly more, without alerting Defendants, then offered the "scraped" information for sale online. There is no indication that Defendants' consumers' PII was removed from the dark web where it likely remains.

27. Not long before CBD admitted hackers were scraping their customers' PII, the FBI issued yet another warning to companies about this exact type of fraud. In the FBI's *Oregon FBI Tech Tuesday: Building a Digital Defense Against E-Skimming*, dated October 22, 2019, the agency stated:

> This warning is specifically targeted to . . . businesses . . . that take credit card payments online. E-skimming occurs when cyber criminals inject malicious code onto a website. The bad actor may have gained access via a phishing attack targeting your employees—or through a vulnerable third-party vendor attached to your company's server.

28. The FBI gave some stern advice to companies like CBD:

> Here's what businesses and agencies can do to protect themselves:
>
> - Update and patch all systems with the latest security software.
> - Anti-virus and anti-malware need to be up-to-date and firewalls strong.
> - Change default login credentials on all systems.
> - Educate employees about safe cyber practices. Most importantly, do not click on links or unexpected attachments in messages.
> - Segregate and segment network systems to limit how easily cyber criminals can move from one to another.

29. But Defendants apparently did not take this advice: hackers scraped customers' PII off CBD's website—and continued to do so until at least May 18, 2020.

30. Web scraping or skimming data breaches are commonly made possible through a vulnerability in a website or their backend content management system. Defendants did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were collecting, causing customers' PII to be exposed and sold on the dark web.

Scraping and E-Skimming Breaches

31. *Magecart* is a loose affiliation of hacker groups responsible for skimming payment card attacks on various companies, including British Airways and Ticketmaster.[7] Typically, these hackers insert virtual credit card skimmers or scrapers (also known as *formjacking*) into a web application (usually the shopping cart), and proceed to scrape credit card information to sell on the dark web.[8]

32. The hackers target what they refer to as the *fullz*—a term used by criminals to refer

[7] *Magecart Hits 80 Major eCommerce Sites in Card-Skimming Bonanza*, Threatpost, Aug. 28, 2019, *available at*: https://threatpost.com/magecart-ecommerce-card-skimming-bonanza/147765/ (last accessed Oct. 7, 2020).
[8] *Id.*

to stealing the full primary account number, card holder contact information, credit card number, CVC code, and expiration date.

33. These cyber-attacks exploit weaknesses in the code of the ecommerce platform, without necessarily compromising the victim website's network or server. These attacks often target third-party payment processors like Shopify or Salesforce.[9]

34. Magecart and these scraping breaches are not new: RiskIQ's earliest Magecart observation occurred on August 8th, 2010.[10] Thus, Defendants would have been made aware of this type of breach since that time, especially considering the surge of these types of breaches in the last few years.

35. Unfortunately, despite all of the publicly available knowledge of the continued compromises of PII in this manner, Defendants' approach to maintaining the privacy and security of Plaintiffs' and Class members' PII was negligent, or, at the very least, Defendants did not maintain reasonable security procedures and practices appropriate to the nature of the information to protect their customers' valuable PII.

Value of Personally Identifiable Information

36. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[11] Experian reports that a stolen credit or debit card number can sell for $5–110 on the dark web; the *fullz* sold for $30 in 2017.[12] Criminals can

[9] *Id.*
[10] *Magecart: New Research Shows the State of a Growing Threat*, RiskIQ, Oct. 4, 2019, *available at*: https://www.riskiq.com/blog/external-threat-management/magecart-growing-threat/ (last accessed Oct. 7, 2020).
[11] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Sept. 30, 2020).
[12] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Sept. 30, 2020).

also purchase access to entire company data breaches from $900 to $4,500.[13]

37. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if their data security system was breached, including, specifically, the significant costs that would be imposed on their customers as a result of a breach.

38. Defendants were, or should have been, fully aware of the significant volume of daily credit and debit card transactions on their website, amounting to thousands of payment card transactions, and thus, the significant number of individuals who would be harmed by a breach of Defendants' systems.

Plaintiff Warshawsky's Experience

39. Plaintiff Warshawsky purchased a product from CBD on April 27, 2020, for a total of $67.48. He used his debit card.

40. On the payment platform, Mr. Warshawsky entered his PII: name, billing address, delivery/billing address, payment card type and full number, CVV security code, payment card expiration date, and email address. During this transaction, Mr. Warshawsky was not asked to "agree" to any "Terms and Conditions" or to review the "Privacy Policy."

41. One month after he made the purchase from CBD, on or about May 28, 2020, Mr. Warshawsky discovered a fraudulent transfer of $1,369.00 from his checking account. To perpetrate the fraud, an unauthorized third party used the same debit card number Mr. Warshawsky used on the cbdMD website on April 27, 2020. The fraudster used a mobile phone app to transfer the funds from Mr. Warshawsky's checking account to an account set up by the fraudster in Mr. Warshawsky's name.

42. Mr. Warshawsky traveled to his bank and started the process to recover the funds. Eventually, the bank determined that the transfer was fraudulent and reimbursed Mr. Warshawsky. As a precaution, Mr. Warshawsky withdrew his money from his checking account and opened a

[13] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Sept. 30, 2020).

new checking account at a different bank. He was forced to change all his electronic payments to the new account. Mr. Warshawsky also had to change the direct deposits from his employer and from the Veterans Administration.

43. On his bank's recommendation, Mr. Warshawsky contacted the Volusia County Sheriff's department to report the crime. The deputy interviewed Mr. Warshawsky at his home. The deputy recommended that Mr. Warshawsky file a complaint with the FBI's Internet Crime Complaint Center, instead of a police report. Mr. Warshawsky filed the complaint online on May 29, 2020.

44. Mr. Warshawsky also had to spend time cancelling the mobile phone app the fraudster opened in his name. Mr. Warshawsky took time out of his day to deal with the fraudulent charges and the bank account change; time he otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life. He also had to use alternative methods of payment until he received his new debit card.

45. On or about September 28, 2020, CBD notified Mr. Warshawsky by U.S. mail of the Data Breaches in the *Notice of Data Breach*.

46. In response to the *Notice of Data Breach*, Mr. Warshawsky again had to spend time dealing with the consequences of the Data Breaches, which includes time reviewing the compromised bank account, contacting his bank, exploring credit monitoring options, and self-monitoring his accounts. Mr. Warshawsky enrolled in the credit monitoring offered by CBD, and routinely monitors the provided updates. This is time Mr. Warshawsky otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

47. Knowing that the hacker stole his PII, and that his PII was and may still be available for sale on the dark web, has caused Mr. Warshawsky great concern. He is now very concerned about credit card theft and financial fraud.

48. Now, due to Defendants' misconduct and the resulting Data Breaches, hackers obtained his PII at no compensation to Mr. Warshawsky whatsoever. That is money lost for him, and money gained for the hackers, who could sell his PII on the dark web.

49. Mr. Warshawsky also suffered actual injury and damages in paying money to, and purchasing products from, Defendants' website during the Data Breaches, expenditures which he would not have made had Defendants disclosed that it lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

50. Moreover, Mr. Warshawsky suffered imminent and impending injury arising from the substantially increased risk of fraud, financial fraud, and misuse resulting from his PII being placed in the hands of criminals.

51. Plaintiff Warshawsky has a continuing interest in ensuring his PII, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Warshawsky' s Efforts to Secure PII

52. Defendants' Data Breaches caused Mr. Warshawsky harm.

53. Prior to the activity described above during the period in which the Data Breaches occurred, the debit card that Mr. Warshawsky used to purchase products on Defendants' website had never been stolen or compromised. Mr. Warshawsky reviewed his credit reports and other financial statements routinely and to his knowledge this card had not been compromised in any manner.

54. Additionally, Mr. Warshawsky never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

55. Mr. Warshawsky stores any and all electronic documents containing his PII in a safe and secure location, and destroys any documents he receives that contain any of his PII, or that may contain any information that could otherwise be used to compromise his payment card. He uses complex passwords for his various online accounts, and routinely changes passwords to enhance security.

Plaintiff Steinhauser's Experience

56. Plaintiff Michael Steinhauser purchased a product from CBD on April 25, 2020, for a total of $65.68. He used his debit card.

57. On the payment platform, Mr. Steinhauser entered his PII: name, billing address,

delivery address, payment card type and full number, CVV security code, payment card expiration date, and email address. He had the product delivered to his mother, supplying CBD with her name and email address. During this transaction, Mr. Steinhauser was not asked to "agree" to any "Terms and Conditions" or to review the "Privacy Policy."

58. After he made the purchase from CBD, on or about July 15, 2020, Mr. Steinhauser was alerted by his bank that someone was charging $452.54 on his debit card at a Best Buy in another city. When the bank alerted Mr. Steinhauser of the purchase, it noted that the debit card being used was his, but the names associated with it were his and his mother's. Mr. Steinhauser contacted his mother, but she did not make the purchase. In fact, Best Buy had emailed Mr. Steinhauser's mother shortly beforehand, telling her an order was ready for pick up. The person designated to pick up the product was unknown to Mr. Steinhauser and his mother. They called Best Buy and put a stop to the transaction, then contacted the bank and had them cancel the charge and change his debit card number.

59. Mr. Steinhauser was forced to change all his electronic payments to the new account. He also filed a police report online with law enforcement. Mr. Steinhauser had to take time out of his day to deal with the fraudulent charges and the debit card number change; time he otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life. He also had to use alternative methods of payment until he received his new debit card.

60. On or about September 28, 2020, CBD notified Mr. Steinhauser by U.S. mail of the Data Breaches in the *Notice of Data Breach*.

61. In response to the *Notice of Data Breach*, Mr. Steinhauser again had to spend time dealing with the consequences of the Data Breaches, which includes time reviewing the account compromised by the Data Breaches, contacting his bank, exploring credit monitoring options, and self-monitoring his accounts. This is time Mr. Steinhauser otherwise would have spent performing other activities, such as his job and/or leisurely activities for the enjoyment of life.

62. Knowing that the hacker stole his PII, and that his PII was and may still be available

for sale on the dark web, has caused Mr. Steinhauser great concern. He is now very concerned about credit card theft and financial fraud.

63. Now, due to Defendants' misconduct and the resulting Data Breaches, hackers obtained his PII at no compensation to Mr. Steinhauser whatsoever. That is money lost for him, and money gained for the hackers, who could sell his PII on the dark web.

64. Mr. Steinhauser also suffered actual injury and damages in paying money to, and purchasing products from, Defendants' website during the Data Breaches, expenditures which he would not have made had Defendants disclosed that it lacked computer systems and data security practices adequate to safeguard customers' PII from theft.

65. Moreover, Mr. Steinhauser suffered imminent and impending injury arising from the substantially increased risk of fraud, financial fraud, and misuse resulting from his PII being placed in the hands of criminals.

66. Plaintiff Steinhauser has a continuing interest in ensuring his PII, which remains in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Steinhauser's Efforts to Secure PII

67. Defendants' Data Breaches caused Mr. Steinhauser harm.

68. Prior to the activity described above during the period in which the Data Breaches occurred, the debit card that Mr. Steinhauser used to purchase products on Defendants' website had never been stolen or compromised. Mr. Steinhauser reviewed his credit reports and other financial statements routinely and to his knowledge this card had not been compromised in any manner.

69. Additionally, Mr. Steinhauser never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

70. Mr. Steinhauser stores any and all electronic documents containing his PII in a safe and secure location, and destroys any documents he receives that contain any of his PII, or that may contain any information that could otherwise be used to compromise his payment card.

CLASS ALLEGATIONS

71. Plaintiffs bring this nationwide class action pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, individually and on behalf of all members of the following class:

> All individuals whose PII was compromised in the Data Breaches announced by CBD on September 25, 2020 (the "Nationwide Class").

72. The Florida Subclass is defined as follows:

> All persons residing in Florida whose PII was compromised in the Data Breaches announced by CBD on September 25, 2020 (the "Florida Subclass").

73. The California Subclass is defined as follows:

> All persons residing in California whose PII was compromised in the Data Breaches announced by CBD on September 25, 2020 (the "California Subclass").

74. Excluded from the Class are the following individuals and/or entities: Defendants and their parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to Defendants' departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as Defendants' immediate family members.

75. Plaintiffs reserve the right to modify or amend the definitions of the proposed Classes before the Court determines whether certification is appropriate.

76. **Numerosity**: The Classes are so numerous that joinder of all members is impracticable. Defendants have identified thousands of customers whose PII may have been improperly accessed in the Data Breaches, and the Classes are apparently identifiable within Defendants' records.

77. **Commonality**: Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class members. These include:

a. When Defendants actually learned of the data breach and whether their response was adequate;

b. Whether Defendants owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, safeguarding and/or obtaining their PII;

c. Whether Defendants breached that duty;

d. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of storing Plaintiffs' and Class members' PII;

e. Whether Defendants acted negligently in connection with the monitoring and/or protection of Plaintiffs' and Class members' PII;

f. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breaches to occur;

h. Whether Defendants caused Plaintiffs and Class members damages;

i. Whether Defendants violated the law by failing to promptly notify Class members that their PII had been compromised;

j. Whether Plaintiffs and the other Class members are entitled to credit monitoring and other monetary relief;

k. Whether Defendants violated Florida's Deceptive and Unfair Trade Practices Act (Florida Statute § 501.203, *et seq.*); and

l. Whether Defendants violated California's Consumer Privacy Act, (Cal. Civ. Code § 1798.100, *et seq*. (§ 1798.150(a)).

78. **Typicality**: Plaintiffs' claims are typical of those of other Class members because all had their PII compromised as a result of the Data Breaches, due to Defendants' misfeasance.

79. **Adequacy**: Plaintiffs will fairly and adequately represent and protect the interests of the Class members. Plaintiffs' Counsel are competent and experienced in litigating privacy-

related class actions.

80. **Superiority and Manageability**: Under 23(b)(3), a class action is superior to other available methods for the fair and efficient adjudication of this controversy since joinder of all the members of the Class is impracticable. Individual damages for any individual Class member are likely to be insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' misconduct would go unpunished. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action.

81. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because Defendants have acted or refused to act on grounds generally applicable to the Class, so that final injunctive relief or corresponding declaratory relief is appropriate as to the Class as a whole.

82. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants owed a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, using, and safeguarding their PII;
b. Whether Defendants breached a legal duty to Plaintiffs and the Class members to exercise due care in collecting, storing, using, and safeguarding their PII;
c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
d. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breaches; and
e. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful

conduct.

FIRST CLAIM FOR RELIEF
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

83. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 82.

84. Defendants owed a duty to Plaintiffs and Class members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

85. The legal duties owed by Defendants to Plaintiffs and Class members include, but are not limited to the following:

a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and Class members in their possession;

b. To protect PII of Plaintiffs and Class members in their possession using reasonable and adequate security procedures that are compliant with industry-standard practices; and

c. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches, including promptly notifying Plaintiffs and Class members of the data breach.

86. Defendants' duty to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45(a), which prohibits "unfair . . . practices in or affecting commerce," including, as interested and enforced by the FTC, the unfair practices of failing to use reasonable measures to protect PII by companies such as Defendant.

87. Various FTC publications and data security breach orders further form the basis of Defendants' duty. Plaintiffs and Class members are consumers under the FTC Act. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with industry standards.

88. Defendants breached their duties to Plaintiffs and Class members. Defendants knew or should have known the risks of collecting and storing PII and the importance of maintaining secure systems, especially in light of the facts that "scraping" hacks have been surging since 2016.

89. Defendants knew or should have known that their security practices did not adequately safeguard Plaintiffs' and the other Class members' PII, including, but not limited to, the failure to detect the malware infecting Defendants' ecommerce platform for months.

90. Through Defendants' acts and omissions described in this Complaint, including Defendants' failure to provide adequate security and their failure to protect the PII of Plaintiffs and the Class from being foreseeably captured, accessed, exfiltrated, stolen, disclosed, accessed, and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' PII during the period it was within Defendants' possession and control.

91. Defendants breached the duties they owe to Plaintiffs and Class members in several ways, including:

a. Failing to implement adequate security systems, protocols, and practices sufficient to protect customers' PII and thereby creating a foreseeable risk of harm;

b. Failing to comply with the minimum industry data security standards during the period of the data breach (*e.g.*, There is no indication that Defendants' ecommerce platform is PCI DSS compliant and encrypts customers' order information, such as name, address, and credit card number, during data transmission, which did not occur here);

c. Failing to act despite knowing or having reason to know that Defendants' systems were vulnerable to E-skimming or similar attacks (*e.g.*, Defendants did not detect the malicious code on the ecommerce platform, nor did they implement safeguards in light of the surge of E-skimming attacks on retailers); and

d. Failing to timely and accurately disclose to customers that their PII had been improperly acquired or accessed and was potentially available for sale to criminals on the dark web.

92. Due to Defendants' conduct, Plaintiffs and Class members are entitled to credit monitoring. Credit monitoring is reasonable here. The PII taken can be used towards identity theft and other types of financial fraud against the Class members. Hackers not only "scraped" many of CBD's customers' names from the website, they also stole customers' billing and shipping addresses, payment card numbers, CVV codes, and payment card expiration dates. They got the *fullz*—everything they need to illegally use CBD's customers' credit cards to make illegal purchases. There is no question that this PII was taken by sophisticated cybercriminals, increasing the risks to the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

93. Some experts recommend that data breach victims obtain credit monitoring services for at least ten years following a data breach. Annual subscriptions for credit monitoring plans range from approximately $219 to $358 per year.

94. As a result of Defendants' negligence, Plaintiffs and Class members suffered injuries that may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from financial fraud and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including but not limited to time spent deleting phishing email messages and cancelling credit cards believed to be associated with the compromised account; (iv) the continued risk to their PII, which may remain for sale on the dark web and is in Defendants' possession, subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of customers and former customers in their continued possession; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and repair the impact of the PII compromised as a result of the

data breach for the remainder of the lives of Plaintiffs and Class members, including ongoing credit monitoring.

95. These injuries were reasonably foreseeable given the history of security breaches of this nature since 2016. The injury and harm that Plaintiffs and the other Class members suffered was the direct and proximate result of Defendants' negligent conduct.

SECOND CLAIM FOR RELIEF
Declaratory Judgment
(On Behalf of Plaintiffs and the Nationwide Class)

96. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 82.

97. Defendants owe duties of care to Plaintiffs and Class members which would require it to adequately secure PII.

98. Defendants still possesses PII regarding Plaintiffs and Class members.

99. Although CBD claims in their *Notice of Data Breach* that it took certain technical precautions to prevent this type of incident from occurring again, there is no detail on what, if any, fixes have really occurred.

100. Plaintiffs and Class members are at risk of harm due to the exposure of their PII and Defendants' failure to address the security failings that lead to such exposure.

101. There is no reason to believe that Defendants' security measures are any more adequate than they were before the breach to meet Defendants' contractual obligations and legal duties, and there is no reason to think Defendants have no other security vulnerabilities that have not yet been knowingly exploited.

102. Plaintiff, therefore, seeks a declaration that (1) each of Defendants' existing security measures do not comply with their explicit or implicit contractual obligations and duties of care to provide reasonable security procedures and practices appropriate to the nature of the information to protect customers' personal information, and (2) to comply with their explicit or

implicit contractual obligations and duties of care, Defendants must implement and maintain reasonable security measures, including, but not limited to:

a. Engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Engaging third-party security auditors and internal personnel to run automated security monitoring;

c. Auditing, testing, and training their security personnel regarding any new or modified procedures;

d. Segmenting their consumer applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Conducting regular database scanning and securing checks;

f. Routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

g. Purchasing credit monitoring services for Plaintiffs and Class members for a period of ten years; and

h. Meaningfully educating their consumers about the threats they face as a result of the loss of their PII to third parties, as well as the steps Defendants' customers must take to protect themselves.

THIRD CLAIM FOR RELIEF
Violation of Florida's Deceptive and Unfair Trade Practices Act, Florida Statute § 501.203, *et seq*.
(On Behalf of Plaintiff Warshawsky and the Nationwide Class, or, in the alternative, On Behalf of Plaintiff Warshawsky and the Florida Subclass)

103. Plaintiff Warshawsky re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 82.

104. Plaintiff Warshawsky and the Florida Subclass Members are "consumers." Fla. Stat. § 501.203(7).

105. Plaintiff Warshawsky and the Florida Subclass Members purchased "things of value" insofar as products and services from Defendants. These purchases were made primarily for personal, family, or household purposes. Fla. Stat. § 501.203(9).

106. Defendants engaged in the conduct alleged in this Complaint by advertising and entering into transactions intended to result, and which did result, in the sale, rental of goods, services, and/or property to consumers, including Plaintiff and the Florida Subclass Members. Fla. Stat. § 501.203(8).

107. Defendants engaged in, and their acts and omissions affected trade and commerce. Defendants' acts, practices, and omissions were done in the course of Defendants' business of advertising, marketing, offering to sell, and selling and/or renting goods and services throughout Florida and the United States. Fla. Stat. § 501.203(8).

108. Defendants, operating in Florida and elsewhere through their worldwide website, engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce, in violation of Fla. Stat. § 501.204(1), including but not limited to the following:

a. charging a premium for the goods and services, implicitly representing that the premium would be used to protect Plaintiff's and Florida Subclass Members' protected health information and other PII;

b. continued acceptance of credit and debit card payments and storage of other PII after Defendants knew or should have known of the Data Breach and before they allegedly remediated the Data Breach.

109. This conduct is considered unfair methods of competition, and constitutes unfair and unconscionable acts and practices. Fla. Stat. § 501.204(1).

110. As a direct and proximate result of Defendants' violation of Florida's Deceptive and Unfair Trade Practices Act ("FDUTPA"), Plaintiff Warshawsky and the Florida Subclass Members suffered actual damages by paying a premium for Defendants' goods and services with the understanding that at least part of the premium would be applied toward sufficient and adequate information security practices that comply with industry standards, when in fact no portion of that premium was applied toward sufficient and adequate information security practices. Fla. Stat. § 501.211(2).

111. Moreover, as a direct result of Defendants' knowing violation of FDUTPA, Plaintiff Warshawsky and the Florida Subclass Members are not only entitled to actual damages, but also declaratory judgment that Defendants' actions and practices alleged herein violate FDUTPA, and injunctive relief, including, but not limited to:

a. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendants audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendants segment PII by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

e. Ordering that Defendants purge, delete, and destroy in a reasonable secure manner PII not necessary for their provisions of services;

f. Ordering that Defendants conduct regular database scanning and securing checks;

g. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. Ordering Defendants to meaningfully educate their customers about the threats they face as a result of the loss of their financial and personal information to third-parties, as well as the steps Defendants' customers must take to protect themselves. Fla. Stat. § 501.211(1).

112. Plaintiff Warshawsky brings this action on behalf of himself and the Florida Subclass Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff and the Florida Subclass Members and the public from Defendants' unfair methods of competition and unfair, deceptive, fraudulent, unconscionable, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

113. The above unfair and deceptive practices and acts by Defendants were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff Warshawsky and the Florida Subclass Members that they could not reasonably avoid; this substantial injury outweighed any benefits to consumers or to competition.

114. Defendants knew or should have known that the lack of encryption on their computer systems and data security practices were inadequate to safeguard the Florida Subclass Members' PII and that the risk of a data disclosure or theft was high.

115. Defendants' actions and inactions in engaging in the unfair practices and deceptive acts described herein were negligent, knowing and willful, and/or wanton and reckless.

116. Plaintiff Warshawsky and the Florida Subclass Members seek relief under Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. §§ 501.201, *et seq.*, including, but not limited to, damages, injunctive relief, and attorneys' fees and costs, and any other just and proper relief.

FOURTH CLAIM FOR RELIEF
Violation of the California Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq*. (§ 1798.150(a)
(On Behalf of Plaintiff Steinhauser and the California Subclass)

117. Plaintiff Steinhauser re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 82.

118. Defendants violated section 1798.150(a) of the California Consumer Privacy Act ("CCPA") by failing to prevent Plaintiff Steinhauser's and California Subclass members' nonencrypted and nonredacted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violations of their duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and California Subclass members.

119. As a direct and proximate result of Defendants' acts, Plaintiff's and the California Subclass members' PII was subjected to unauthorized access and exfiltration, theft, or disclosure as a result of Defendants' violation of the duty: through CBD's website, the ecommerce platform, and/or from the dark web, where hackers further disclosed ("as a result of [Defendants'] violation of the duty") CBD's consumers' PII.

120. As a direct and proximate result of Defendants' acts, Plaintiff and the California Subclass members were injured and lost money or property, including but not limited to the price received by Defendants for the products, the loss of California Subclass members' legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as described above.

121. Defendants knew or should have known that Defendants' computer systems and data security practices were inadequate to safeguard California Subclass members' PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII of Plaintiff and the California Subclass members.

122. CBD is organized or operated for the profit or financial benefit of CBD's owners/shareholders, with annual gross revenues over $25 million. CBD collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

123. Plaintiff and California Subclass members seek relief under § 1798.150(a), including, but not limited to, recovery of actual damages; injunctive or declaratory relief; any other relief the court deems proper; and attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5).

124. Plaintiff and the California Subclass members reserve the right to amend this Complaint as of right to seek statutory damages and relief under Cal. Civ. Code § 1798.100, *et seq*.

FIFTH CLAIM FOR RELIEF
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class)

125. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 82.

126. Plaintiffs and class members conferred a monetary benefit upon Defendants in the form of monies paid for goods available on Defendants' websites.

127. Defendants appreciated or had knowledge of the benefits conferred upon them by Plaintiffs and Class members. Defendants also benefited from the receipt of Plaintiffs' and Class members' PII, as this was used by Defendants to facilitate payment to them.

128. The monies for goods that Plaintiffs and Class members paid to Defendants were to be used by Defendant, in part, to pay for the administrative costs of reasonable data privacy and security practices and procedures.

129. As a result of Defendants' conduct, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their purchases made with reasonable data privacy and security practices and procedures that Plaintiffs and Class members

paid for, and those purchases without unreasonable data privacy and security practices and procedures that they received.

130. Under principals of equity and good conscience, Defendants should not be permitted to retain the money belonging to Plaintiffs and Class members because Defendants failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

131. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds received by it as a result of the conduct alleged herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class members, request judgment against Defendants and that the Court grant the following:

A. An order certifying the Nationwide Class, Florida Subclass, and California Subclass as defined herein, and appointing Plaintiffs and their counsel to represent the classes;

B. An order enjoining Defendants from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs' and Class members' PII;

C. An order instructing Defendants to purchase or provide funds for credit monitoring services for Plaintiffs and all Class members;

D. An award of compensatory, statutory, nominal and punitive damages, in an amount to be determined at trial;

E. An award for equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: October 9, 2020

Respectfully Submitted,

By: */s/ Jean Sutton Martin*

JEAN MARTIN
JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN J. MCGEE
(*Pro Hac Vice application forthcoming*)
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
jeanmartin@ForThePeople.com
rmcgee@ForThePeople.com

M. ANDERSON BERRY
(*Pro Hac Vice application forthcoming*))
LESLIE GUILLON
(*Pro Hac Vice application forthcoming*))
CLAYEO C. ARNOLD,
A PROFESSIONAL LAW CORP.
865 Howe Avenue
Sacramento, CA 95825
(916) 777-7777
aberry@justice4you.com
lguillon@justice4you.com

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

MICAHEL WARSHAWSKY and MICHAEL STEINHAUSER

(b) County of Residence of First Listed Plaintiff _____
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor, Tampa, Florida 33602

DEFENDANTS

CDBMD, INC. and CBD INDUSTRIES, LLC,

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☒ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☒ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332(d)

Brief description of cause:
Negligence, Declaratory Judgment, Violation of Florida's Deceptive and Unfair Trade Practices Act, Violation of the California Consumer Privacy Act

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $ 5000000

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY *(See instructions)*: JUDGE _____ DOCKET NUMBER _____

DATE
10/09/2020

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

UNITED STATES DISTRICT COURT
for the
Western District of North Carolina

MICAHEL WARSHAWSKY and MICHAEL STEINHAUSER, behalf of themselves and all others similarly situated,

Plaintiff

v.

Civil Action No.

CDBMD, INC. and CBD INDUSTRIES, LLC,

Defendant

SUMMONS IN A CIVIL ACTION

TO: ***(Defendant's name and address)***

CDBMD, INC.
8845 Red Oak Boulevard
Charlotte, NC 28217

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) – or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12(a)(2) or (3) – you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

JEAN MARTIN
MORGAN & MORGAN
COMPLEX LITIGATION GROUP
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4(1))

This summon for *(name of individual and title, if any)*
_____
was received by me on *(date)* _____.

❑ **I personally served the summons on the defendant at *(place)*_____ on *(date)* _____; or**

❑ **I left the summons at the individual's residence or usual place of abode with *(name)* _____, a person of suitable age and discretion who resides there, on *(date)* _____, and mailed a copy to the individual's last known address; or**

❑ **I served the summons on *(name of individual)* _____, who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____; or**

❑ **I returned the summons unexecuted because _____; or**

❑ **Other *(specify)*:**
_____

My fees are $ _____ for travel and $ _____ for services, for a total of $_____.

I declare under penalty of perjury that this information is true.

Date:_____ **_____**
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc: