CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
rclarkson@clarksonlawfirm.com
Yana Hart (SBN 306499)
yhart@clarksonlawfirm.com
Tiara Avaness (SBN 343928)
tavaness@clarksonlawfirm.com
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Fax: (213) 788-4070

Counsel for Plaintiff and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

AQUELIA WALKER, on behalf of herself and all others who are similarly situated,

Plaintiff,

v.

DROPBOX, INC.

Defendant.

Case No. 3:24-cv-2659

CLASS ACTION COMPLAINT

1. **NEGLIGENCE**
2. **NEGLIGENCE PER SE**
3. **BREACH OF FIDUCIARY DUTY**
4. **UNJUST ENRICHMENT**
5. **BREACH OF IMPLIED CONTRACT**
6. **VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 Cal. Civ. Code §§ 1798.100 et seq. ("CCPA")**
7. **VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT Cal. Civ. Code §§ 1750 et seq. ("CLRA")**
8. **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW Cal. Bus. and Prof. Code §§ 17200, et seq. ("UCL")**

DEMAND FOR JURY TRIAL

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

CLASS ACTION COMPLAINT

Plaintiff Aquelia Walker ("**Plaintiff**") individually and on behalf of all others similarly situated, brings this Class Action Complaint (the "**Complaint**"), and alleges the following against Defendant Dropbox, Inc. ("Dropbox" or **Defendant**"), based upon personal knowledge with respect to herself and upon information and belief derived from, among other things, investigation of counsel and review of public documents as to all other matters.

NATURE OF THE ACTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard Plaintiff and other similar situated individuals' personal identifiable information ("**PII**"), including but not limited to "emails, usernames, phone numbers and hashed passwords, in addition to general account settings and certain authentication information such as API Keys, OAuth tokens, and multi-factor authentication" (collectively, "**Private Information**").[1]

2. This class action arises out of the recent targeted cyberattack against Dropbox that enabled a third party to access Defendant's computer systems and data, resulting in the compromise of highly sensitive PII (the "**Data Breach**").[2]

3. Due to the Data Breach, Plaintiff and Class Members suffered ascertainable losses in the form of the benefit of their bargain, out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack, emotional distress, and the imminent risk of future harm caused by the compromise of their Private Information.

---

[1] DropBox Sign Team, *A Recent Security Incident Involving Dropbox Sign,* DROPBOX SIGN (May 1, 2024), https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign (Last accessed May 2, 2024).

[2] Lawrence Abrams, *Dropbox Says Hackers Stole Customer Data, Auth Secrets from eSignature Service*, BLEEPINGCOMPUTER (May 1, 2024), https://www.bleepingcomputer.com/news/security/dropbox-says-hackers-stole-customer-data-auth-secrets-from-esignature-service/; Newsroom, *Dropbox Discloses Breach of Digital Signature Service Affecting All Users*, THE HACKER NEWS (May 2, 2024), https://thehackernews.com/2024/05/dropbox-discloses-breach-of-digital.html; Eduard Kovacs, *Hackers Compromised Dropbox eSignature Service*, SECURITYWEEK (May 2, 2024), https://www.securityweek.com/dropbox-data-breach-impacts-customer-information/. (Last accessed May 2, 2024)

4. The Data Breach was a direct result of Dropbox's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect consumers' Private Information.

5. On or around April 24, 2024, Dropbox became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment.[3] Upon further investigation, Dropbox discovered that a threat actor had accessed customer information.[4]

6. This was not a passive data breach where, for example, it is unclear whether the compromised data was targeted or even seen. Here, the Data Breach occurred because Dropbox enabled an unauthorized third party to gain access to and obtain former and current Dropbox customers' Private Information from Dropbox internal computer systems.[5]

7. Defendant's Notice failed to disclose how it discovered the encrypted files on its computer systems were impacted, the means and mechanisms of the cyberattack, the reason for the delay in notifying Plaintiff and the Class of the Data Breach, how Defendant determined that the Private Information had been "accessed" by an unauthorized party. However, Dropbox did concede that, based on its own investigation:

> "[A] third party gained access to a Dropbox Sign automated system configuration tool. The actor compromised a service account that was part of Sign's back-end, which is a type of non-human account used to execute applications and run automated services. As such this account had privileges to take a variety of actions within Sign's production environment. The threat actor then used this access to the production environment to access our customer database."[6]

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

---

[3] DropBox Sign Team, *A Recent Security Incident Involving Dropbox Sign,* DROPBOX SIGN (May 1, 2024), https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign (Last accessed May 2, 2024).

[4] *Id.*

[5] *Id.*

[6] DropBox Sign Team, *A Recent Security Incident Involving Dropbox Sign,* DROPBOX SIGN (May 1, 2024), https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign (last accessed May 2, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

9. By being entrusted with Plaintiff's and class members' PII for its own pecuniary benefit, Dropbox assumed a duty to Plaintiff and Class Members to implement and maintain reasonable and adequate security measures to secure, protect, and safeguard Plaintiff's and Class Members' Private Information against unauthorized access and disclosure.

10. Dropbox also had a duty to adequately safeguard this Private Information under controlling case law, as well as pursuant to industry standards and duties imposed by statutes, including Section 5 of the Federal Trade Commission Act (the "**FTC Act**").

11. Dropbox breached those duties by and disregarded the rights of Plaintiff and the Class Members by intentionally, willfully, recklessly, or negligently failing to implement proper and reasonable measures to safeguard consumers' PII; failing to take available and necessary steps to prevent unauthorized disclosure of data; and failing to follow applicable, required, and proper protocols, policies, and procedures regarding the encryption of data.

12. As a result of Dropbox's inadequate security and breach of its duties and obligations, the PII of Plaintiff and Class Members was compromised through disclosure to an unauthorized criminal third party. Plaintiff and Class Members have suffered injuries as a direct and proximate result of Defendant's conduct. These injuries include: (i) diminution in value and/or lost value of PII, a form of property that Dropbox obtained from Plaintiff and Class Members; (ii) out-of-pocket expenses associated with preventing, detecting, and remediating identity theft, social engineering, and other unauthorized use of their PII; (iii) opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term, and certain increased risk that unauthorized persons will access and abuse Plaintiff's and Class Members' PII; (v) the continued and certain increased risk that the PII 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 PII; (v) invasion of privacy and increased risk of fraud and identity theft; and (vi) theft of their PII and the resulting loss of privacy rights in that information. This action seeks to remedy these failings and their consequences. Plaintiff and Class Members have a continuing interest

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

in ensuring that their PII is and remains safe, and they should be entitled to injunctive and other equitable relief.

13. The injury to Plaintiff and Class Members was compounded by the fact that Dropbox did not immediately notify those affected that their Private Information was subject to unauthorized access and exfiltration until May 2024.

14. Dropbox's failure to timely notify the victims of its Data Breach prevented Plaintiff and Class Members from taking swift affirmative measures to prevent or mitigate the resulting harm, including but not limited to changing their passwords and monitoring accounts for unauthorized activity.

15. Despite having been accessed and exfiltrated by unauthorized criminal actors, Plaintiff's and Class Members' sensitive and confidential PII remains in the possession of Dropbox. Absent additional safeguards and independent review and oversight, the information remains vulnerable to further cyberattacks and theft. The aggregate data compromised in the Data Breach, taken as a whole, including but limited to names, emails, phone numbers, hashed passwords, and authentication information, increases the risk of harm, making identity theft a likely outcome.

16. Dropbox disregarded the rights of Plaintiff and Class Members by, *inter alia*, failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard PII; failing to take standard and reasonably available steps to prevent the Data Breach; failing to properly train its staff and employees on proper security measures; and failing to provide Plaintiff and Class Members prompt and adequate notice of the Data Breach.

17. In addition, Dropbox failed to properly monitor the computer network and systems that housed the PII. Had Dropbox properly monitored these electronic systems, Dropbox would have discovered the intrusion sooner or prevented it altogether.

18. The security of Plaintiff's and Class Members' identities is now at substantial risk because of Dropbox's wrongful conduct as the PII that Defendant collected and maintained are now in the hands of data thieves. This present risk will continue for the course of their lives.

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

19. Armed with the PII accessed in the Data Breach, data thieves can commit a wide range of crimes.

20. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a present and imminent risk of fraud and identity theft. Among other measures, Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft. Further, Plaintiff and Class Members will incur out-of-pocket costs to purchase adequate credit monitoring and identity theft protection and insurance services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

21. Plaintiff and Class Members will also be forced to expend additional time to review credit reports and monitor their financial accounts for fraud or identity theft. And because the exposed other immutable personal details, the risk of identity theft and fraud will persist throughout their lives.

22. Plaintiff brings this lawsuit on behalf of herself and all of those similarly situated to address Dropbox's inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was unsecured and subjected to the unauthorized access of any unknown third party.

23. Plaintiff, on behalf of herself and all other Class Members, brings claims for negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, and for declaratory and injunctive relief. To remedy these violations of law, Plaintiff and Class Members thus seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including significant improvements to Dropbox'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.

///

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because: (i) the amount in controversy exceeds $5 million, exclusive of interest and costs; (ii) the number of class members exceeds 100 and (iii) minimal diversity exists because many class members, including Plaintiff has different citizenship from Defendant.

25. This Court has personal jurisdiction over Defendant because Defendant has purposefully availed itself of the laws, rights, and benefits of the State of California. Defendant is headquartered in California and has engaged in activities including (i) directly and/or through its parent companies, affiliates and/or agents providing services throughout the United States in this judicial district; (ii) conducting substantial business in this forum; and/or (iii) engaging in other persistent courses of conduct and/or deriving substantial revenue from services provided in California and in this judicial District.

26. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events giving rise to this action occurred in this District. Moreover, Defendant is based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members in this District.

PARTIES

Plaintiff Aquelia Walker

27. Plaintiff Aquelia Walker ("**Plaintiff**") is a citizen of the State of California. At all relevant times, Plaintiff has resided in Clovis, California.

28. For the past three years, Plaintiff has been Defendant's customer and Dropbox account holder. Plaintiff provided her PII to Defendant. In receiving and maintaining her PII for its business purposes, Defendant expressly and impliedly promised, and undertook a duty, to act reasonably in its handling of Plaintiff's Private Information. Defendant, however, did not take proper care of Plaintiff's Private Information, leading to its exposure to and exfiltration by cybercriminals as a direct result of Defendant's inadequate cybersecurity measures.

29. On May 1, 2024, Plaintiff received notice of the Data Breach via email. Deeply concerned and troubled, Plaintiff immediately went to the internet to investigate the Data Breach because Plaintiff

was (and continues to be) worried about her PII being readily available for cybercriminals to sell, buy, and exchange, even on the Dark Web.

30. Since receiving the notice of the Data Breach, Plaintiff has spent over five hours to determine the extent and gravity of the Data Breach.

31. Plaintiff is especially concerned because she believes she may have used Dropbox as recently as April 4, 2024, thus giving cybercriminals unauthorized access to her most recent personal information.

32. Plaintiff's main concern is her stolen identity and individuals pretending to be her when they are not.

Defendant Dropbox, Inc.

33. Defendant Dropbox, Inc. is a Delaware corporation headquartered in California with its principal executive office located at 1800 Owens Street, Suite 200, San Francisco, California 94518.

34. Dropbox is a publicly traded technology company, with a net worth of over $8.08 billion.

35. Dropbox "offers cloud storage, file synchronization, file sharing and client software services…[Dropbox] provides solutions to securely store, synchronize, and share business files. It enables editing, adding, and transferring files across devices securely…[and] allows business to protect their users' documents preventing entering other mobile or web devices."[7]

36. Plaintiff and Class Members are current and former customers of Dropbox.

37. Due to the nature of the services Dropbox provides, it receives and is entrusted with securely storing consumers' Private Information, which includes, inter alia, individuals' full name, date of birth, and other sensitive information. Defendant promised to provide confidentiality and adequate security for the data it collected from customers through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

///

///

[7] GlobalData, *Dropbox Inc: Company Profile*, GLOBALDATA, N.D., https://www.globaldata.com/company-profile/dropbox-inc/. (Last accessed May 2, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

FACTUAL ALLEGATIONS

A. The Data Breach, Dropbox's Unsecure Data Management, and Disclosure of Data Breach.

38. On or about April 24, 2024, Dropbox reported that a hacker breached company systems and gained access to sensitive information like passwords and more.[8]

39. On May 1, 2024, Dropbox filed an 8-K Form with the Securities and Exchange Commission detailing a "material cybersecurity incident."[9] This 8-K disclosure states:

> "On April 24, 2024, Dropbox, Inc. ("*Dropbox"* or "*we*") became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment. We immediately activated our cybersecurity incident response process to investigate, contain, and remediate the incident. Upon further investigation, we discovered that the threat actor had accessed data related to all users of Dropbox Sign, such as emails and usernames, in addition to general account settings. For subsets of users, the threat actor also accessed phone numbers, hashed passwords, and certain authentication information such as API keys, OAuth tokens, and multi-factor authentication."[10]

40. The threat actor was able to gain access to "a Dropbox Sign automated system configuration tool, which is part of the platform's backend services."[11] This tool enabled the threat actor to "execute applications and automated services with elevated privileges, allowing the attacker to access

---

[8] Jonathan Greig, *Dropbox Says Hacker Accessed Passwords, Authentication Info During Breach*, THE RECORD (May 1, 2024), https://therecord.media/dropbox-data-breach-notification. (Last accessed May 2, 2024); DropBox Sign Team, *A Recent Security Incident Involving Dropbox Sign,* DROPBOX SIGN (May 1, 2024), https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign (last accessed May 2, 2024).

[9] Dropbox, Inc., *Form 8-K Current Report*, U.S. SECURITIES AND EXCHANGE COMMISSION (April 29, 2024), https://www.sec.gov/Archives/edgar/data/1467623/000146762324000024/dbx-20240429.htm. (Last accessed May 2, 2024).

[10] *Id.*

[11] Lawrence Abrams, *Dropbox Says Hackers Stole Customer Data, Auth Secrets from eSignature Service*, BLEEPINGCOMPUTER (May 1, 2024), https://www.bleepingcomputer.com/news/security/dropbox-says-hackers-stole-customer-data-auth-secrets-from-esignature-service/. (Last accessed May 2, 2024)

the customer database."[12] Beyond the customer database, the email addresses and names of users who simply used the eSignature platform without an account were also exposed.[13]

41. Prior to the Data Breach in April 2024, Plaintiff and Class Members had provided their Private Information to Dropbox with the reasonable expectation and mutual understanding that Dropbox would comply with its obligations to keep such information confidential and secure from unauthorized access. In particular, Plaintiff and Class Members provided their names, emails, and phone numbers to Dropbox in order to register for an account and utilize Dropbox Sign.

42. Additionally, Plaintiff and Class Members' account authentication information, such as "API keys, OAuth tokens, and multi-factor authentication,"[14] was compromised. With this information, the threat actor had access to users' accounts, which stored sensitive documents and agreements, as well as payment information.

43. Dropbox Sign's sole product offering is a service to upload "legally-binding eSignatures" so users can "execute business critical documents."[15] This service is essential for users, such as Plaintiff and Class Members, who rely on the integrity and confidentiality of their "business critical documents." The Data Breach has not only compromised PII but gave a threat actor access to sensitive business documents deemed crucial for business operations.

44. PII is a valuable property right.[16] "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the

[12] *Id.*
[13] *Id.*
[14] Dropbox, Inc., *Form 8-K Current Report*, U.S. Securities and Exchange Commission (April 29, 2024), https://www.sec.gov/Archives/edgar/data/1467623/000146762324000024/dbx-20240429.htm.
[15] Dropbox, Inc., *Dropbox Sign*, DROPBOX, N.D., https://www.dropbox.com/sign. (Last accessed May 2, 2024)
[16] *See* Marc van Lieshout, The Value of Personal Data, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY 26 (May 2015), https://www.researchgate.net/publication/283668023_ The_Value_of_Personal_Data ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible...").

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

existing legal and regulatory frameworks."[17] It is estimated that American companies have spent over $19 billion on acquiring personal data of consumers in 2018.[18] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

45. Upon information and belief, Plaintiff and the Class's Private Information exposed in the Data Breach has been exposed on the Dark Web.

46. Dropbox promised consumers it would keep their data secure and private. Data security is purportedly a critical component of Dropbox's business model. On a section of its website, Dropbox makes the following statements:

> "We have a team dedicated to keeping your information secure and testing for vulnerabilities. We continue to work on features to keep your information safe in addition to things like two-factor authentication, encryption of files at rest, and alerts when new devices and apps are linked to your account. We deploy automated technologies to detect abusive behavior and content that may harm our Services, you, or other users."[19]

47. On its website, Dropbox also maintains a "Data Privacy Frameworks" section, stating its compliance with the various data privacy frameworks and laws of the United States.[20]

48. Contrary were Dropbox's various express assurances that it would take reasonable measures to safeguard the sensitive information entrusted to it – and only share it for an express authorized persons – an "unauthorized" person or persons was able to access its network servers.

49. To date, Dropbox has not disclosed complete specifics of the attack, such as whether ransomware has been used.

50. As such, Dropbox failed to secure the PII of the individuals that provided it with

---

[17] *Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value*, OECD 4 (Apr. 2, 2013), https://www.oecd-ilibrary.org/science-and-technology/exploring-the-economics-of-personal-data_5k486qtxldmq-en

[18] U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/.

[19] Dropbox, Inc., *Privacy Policy*, DROPBOX (Sep. 26, 2023), https://www.dropbox.com/privacy. (Last accessed May 2, 2024).

[20] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

this sensitive information. It failed to take appropriate steps to protect the PII of Plaintiff and other Class Members from being disclosed.

B. Dropbox Failed to Comply with FTC Guidelines

51. Dropbox was prohibited by the Federal Trade Commission Act (the "**FTC Act**") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission (the "**FTC**") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, FTC v. Wyndham Worldwide Corp., 799 F.3d 236 (3d Cir. 2015).

52. The FTC has promulgated numerous guides for businesses which 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.

53. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer 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.[21] 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 being transmitted from the system; and have a response plan ready in the event of a breach.[22]

54. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; 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.

[21] Federal Trade Commission, *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business. (Last accessed May 2, 2024).

[22] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

55. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer 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.

56. These FTC enforcement actions include actions against healthcare providers and partners like Dropbox. *See, e.g.*, In the Matter of Labmd, Inc., A Corp, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.")

57. Dropbox failed to properly implement basic data security practices, allowing for this attack to occur, victimizing millions of people.

58. Dropbox's failure to employ reasonable and appropriate measures to protect against unauthorized access to customers' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

59. Dropbox was at all times fully aware of the obligation to protect the Private Information of customers and patients. Dropbox was also aware of the significant repercussions that would result from its failure to do so.

60. Dropbox is no stranger to data breaches, as its lax security practices have resulted in multiple disclosures of consumers' sensitive personal information. In 2011, just three years after it was founded, Dropbox's systems experienced a bug that would allow anyone to access any account with just the username or email.[23] In 2012, Dropbox accounts were subject to unauthorized access with stolen usernames and passwords, which resulted in attackers gaining access to Dropbox systems.[24] **Only four years later**, in 2016, did the public learn that approximately 68 million users had been compromised in

[23] Fergus O'Sullivan, *A Timeline of Dropbox Security Issues*, PROTON BLOG (January 26, 2024), https://proton.me/blog/dropbox-security-issues. (Last accessed, May 2, 2024).
[24] *Id.*

the 2012 Dropbox incident, making it the "biggest hack in cloud storage history."[25] Recently, in 2022, Dropbox employee credentials were stolen during a phishing attack.[26]

C. Plaintiff and the Class Have Suffered Injury as a Result of Dropbox's Data Mismanagement

61. As a result of Dropbox's failure to implement and follow even the most basic security procedures, Plaintiff and Class Members' PII have been and are now in the hands of an unauthorized third-party which may include thieves, unknown criminals, banks, credit companies, and other potentially hostile individuals. Plaintiff and other Class Members now face an increased risk of identity theft and will consequentially have to spend, and will continue to spend, significant time and money to protect themselves due to Dropbox's Data Breach.

62. Plaintiff and other Class Members have had their most personal and sensitive Private Information disseminated to the public at large and have experienced and will continue to experience emotional pain and mental anguish and embarrassment.

63. Plaintiff and Class Members face an increased risk of identity theft, phishing attacks, and related cybercrimes because of the Data Breach. Those impacted are under heightened and prolonged anxiety and fear, as they will be at risk for falling victim for cybercrimes for years to come.

64. PII is a valuable property right.[27] The value of PII as a commodity is measurable. "Firms are now able to attain significant market valuations by employing business models predicated on the successful use of personal data within the existing legal and regulatory frameworks."[28] American companies are estimated to have spent over $19 billion on acquiring personal data of consumers in

[25] *Id.*
[26] *Id.*
[27] *See,* Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND COMMUNICATION TECHNOLOGY (May 2015), https://www.researchgate.net/publication/283668023 ("The value of [personal] information is well understood by marketers who try to collect as much data about personal conducts and preferences as possible..."). (Last accessed May 2, 2024).
[28] *See,* Robert Lowes, *Stolen EHR [Electronic Health Record] Charts Sell for $50 Each on Black Market*, MEDSCAPE (Apr. 28, 2014), http://www.medscape.com/viewarticle/824192 .(Last accessed May 2, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

2018.[29] It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on the "cyber black-market," or the "dark web," for many years.

65. As a result of its real value and the recent large-scale data breaches, identity thieves and cyber criminals have openly posted credit card numbers, Social Security numbers, PII, and other sensitive information directly on various Internet websites, making the information publicly available. This information from various breaches, including the information exposed in the Data Breach, can be aggregated, and become more valuable to thieves and more damaging to victims.

66. Personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[30] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web. Criminals can also purchase access to entire company data breaches from $900 to $4,500.[31]

67. Consumers place a high value on the privacy of that data. Researchers shed light on how many consumers value their data privacy—and the amount is considerable. Indeed, studies confirm that "when privacy information is made more salient and accessible, some consumers are willing to pay a premium to purchase from privacy protective websites."[32]

68. Given these facts, any company that transacts business with a consumer and then compromises the privacy of consumers' PII has thus deprived that consumer of the full monetary value of the consumer's transaction with the company.

---

[29] *U.S. Firms to Spend Nearly $19.2 Billion on Third-Party Audience Data and Data-Use Solutions in 2018, Up 17.5% from 2017*, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018), https://www.iab.com/news/2018-state-of-data-report/ (Last accessed May 2, 2024).

[30] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs*, DIGITAL TRENDS (Oct. 16, 2019), accessible at https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs// (Last accessed May 2, 2024).

[31] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), accessible at https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (Last accessed May 2, 2024).

[32] Janice Y. Tsai et al., *The Effect of Online Privacy Information on Purchasing Behavior, An Experimental Study*, 22(2) INFORMATION SYSTEMS RESEARCH 254 (June 2011), accessible at https://www.jstor.org/stable/23015560?seq=1 (Last accessed May 2, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

69. Cyberattacks have become so notorious that the FBI and U.S. Secret Service have issued a warning to potential targets, so they are aware of, and prepared for, a potential attack. As one report explained, "[e]ntities like smaller municipalities and hospitals are attractive to ransomware criminals... because they often have lesser IT defenses and a high incentive to regain access to their data quickly.[33]

70. Plaintiff and members of the Class must immediately devote time, energy, and money to: 1) closely monitor their bills, records, and credit and financial accounts; 2) change login and password information on any sensitive account even more frequently than they already do; 3) more carefully screen and scrutinize phone calls, emails, and other communications to ensure that they are not being targeted in a social engineering or spear phishing attack; and 4) search for suitable identity theft protection and credit monitoring services, and pay to procure them.

71. Once PII is exposed, there is virtually no way to ensure that the exposed information has been fully recovered or contained against future misuse. For this reason, Plaintiff and Class Members will need to maintain these heightened measures for years, and possibly their entire lives, because of Dropbox's conduct. Further, the value of Plaintiff's and Class Members' Private Information has been diminished by its exposure in the Data Breach.

72. As a result of Dropbox's failures, Plaintiff and Class Members are at substantial risk of suffering identity theft and fraud or misuse of their Private Information.

73. Plaintiff and members of the Class suffered actual injury from having PII compromised as a result of Dropbox's negligent data management and resulting Data Breach including, but not limited to (a) damage to and diminution in the value of their PII, a form of property that Dropbox obtained from Plaintiff; (b) violation of their privacy rights; and (c) present and increased risk arising from the identity theft and fraud.

74. For the reasons mentioned above, Dropbox's conduct, which allowed the Data Breach to occur, caused Plaintiff and members of the Class these significant injuries and harm.

[33] Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019), accessible at https://www.law360.com/articles/1220974 (Last accessed May 2, 2024).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

75. Plaintiff brings this class action against Dropbox for their failure to properly secure and safeguard Private Information and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their Private Information had been compromised.

76. Plaintiff, individually and on behalf of all other similarly situated individuals, alleges claims in negligence, negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, violations of the California Consumer Privacy Act and California Legal Remedies Act, and California's Unfair Competition Law.

CLASS ACTION ALLEGATIONS

77. Plaintiff brings this action on behalf of herself and on behalf of all other persons similarly situated ("**the Class**").

78. Plaintiff proposes the following Class and Subclass definitions, subject to amendment(s) as appropriate:

Nationwide Class

> All individuals residing in the United States whose Private Information was compromised as a result of the Data Breach, including all individuals who were sent a notice of the Data Breach ("**the Class**").

California Subclass

> All individuals identified by Defendant (or its agents or affiliates) as being those persons residing in California impacted by the Data Breach, including all who were sent a notice of the Data Breach (the "**California Subclass**").

79. Collectively, the Class and California Subclass are referred to as the Classes.

80. Excluded from the Class are Dropbox's officers and directors, and any entity in which Dropbox has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Dropbox. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

81. Plaintiff reserves the right to amend or modify the Class or Subclass definitions as this case progresses.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

82. **Numerosity:** Upon information and belief, the members of the Class are so numerous that joinder of all of them is impracticable.

83. Existence/Predominance of Common Questions of Fact and Law: There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Dropbox unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' PII;

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

c. Whether Dropbox's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Dropbox's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Dropbox owed a duty to Class Members to safeguard their PII;

f. Whether Dropbox was subject to (and breached) the FTC Act, the California Confidentiality of Medical Information Act and/or the CCPA;

g. Whether Dropbox breached its duty to Class Members to safeguard their PII;

h. Whether computer hackers obtained Class Members' PII in the Data Breach;

i. Whether Dropbox knew or should have known that its data security systems and monitoring processes were deficient;

j. Whether Dropbox's conduct was negligent;

k. Whether Dropbox's acts breaching an implied contract they formed with Plaintiff and the Class Members;

l. Whether Dropbox was unjustly enriched to the detriment of Plaintiff and the Class;

m. Whether Dropbox failed to provide notice of the Data Breach in a timely manner; and

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

n. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

84. **Typicality:** Plaintiff's claims are typical of those of other Class Members because Plaintiff's PII, like that of every other Class Member, was compromised in the Data Breach.

85. **Adequacy:** Plaintiff is an adequate representative for the Class because his interests do not conflict with the interests of the Class that he seeks to represent. Plaintiff has retained counsel competent and highly experienced in complex class action litigation—including consumer fraud and automobile defect class action cases—and counsel intends to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his experienced counsel.

86. **Superiority:** A class action is superior to all other available means of fair and efficient adjudication of the claims of Plaintiff and members of the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Dropbox's conduct. It would be virtually impossible for members of the Class individually to redress effectively the wrongs done to them by Dropbox. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, an economy of scale, and comprehensive supervision by a single court. Upon information and belief, members of the Class can be readily identified and notified based upon, inter alia, the records (including databases, e-mails, dealership records and files, etc.) Dropbox maintains regarding their consumers.

87. Defendant has acted, and refuses to act, on grounds generally applicable to the Class, thereby making appropriate final equitable relief with respect to the Class as a whole.

///

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

CALIFORNIA LAW SHOULD BE APPLIED TO THE NATIONWIDE CLASS

88. The State of California has a significant interest in regulating the conduct of businesses operating within its borders. California seeks to protect the rights and interests of all California residents and citizens of the United States against a company headquartered and doing business in California. California has a greater interest in the nationwide claims of Plaintiff and members of the Class than any other state and is most intimately concerned with the claims and outcome of this litigation. *See Ehret v. Uber Techs., Inc.*, 68 F.Supp.3d 1121, 1130 (N.D. Cal. 2014) (noting courts including the California Supreme Court have permitted the application of California law in cases where alleged misrepresentations were "disseminated from California"); *In re Toyota Motor Corp.*, 785 F.Supp.2d 883, 917 (C.D. Cal. 2011) (To determine whether California law should apply, "courts consider where the defendant does business, whether the defendant's principal offices are located in California, where class members are located, and the location from which advertising and other promotional literature decisions were made.").

89. Defendant is located in California and conducts substantial business in California, such that California has an interest in regulating Defendant's conduct under its laws. The corporate headquarters of Defendant are in California which is the "nerve center" of its business activities – the place where its officers direct, control, and coordinate the company's activities, including its data security functions and policy, financial, and legal decisions. Further, upon information and belief, all managerial decisions stem from California, the representations on Defendant's website originate from California, and Defendant's response to the Data Breach, and corporate decisions surrounding such response, was made from California. Therefore, application of California law to the Class is appropriate. The flawed cybersecurity measures that led to the Data Breach were developed and managed from California. All of Defendant's contracts and agreements pertaining to the data security services and protocols in question are executed in California.

90. Defendant's decision to conduct substantial business in California and avail itself of California's laws, renders the application of California law to the claims herein constitutionally permissible.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

CLAIMS FOR RELIEF

COUNT 1

NEGLIGENCE

(On Behalf of Plaintiff and the Nationwide Class)

91. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

92. Dropbox owed a duty to Plaintiff and all other Class Members to exercise reasonable care in safeguarding and protecting their PII in its possession, custody, or control.

93. Dropbox knew, or should have known, the risks of collecting and storing Plaintiff's and all other Class Members' PII and the importance of maintaining secure systems. Dropbox knew, or should have known, of the vast uptick in data breaches in recent years. Dropbox had a duty to protect the PII of Plaintiff and Class Members.

94. Given the nature of Dropbox's business, the sensitivity and value of the PII it maintains, and the resources at its disposal, Dropbox should have identified the vulnerabilities to its systems and prevented the Data Breach from occurring, which Dropbox had a duty to prevent.

95. Dropbox breached these duties by failing to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing 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 PII entrusted to it—including Plaintiff's and Class Members' PII.

96. It was reasonably foreseeable to Dropbox that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems would result in the unauthorized release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

97. But for Dropbox's negligent conduct or breach of the above-described duties owed to Plaintiff and Class Members, their PII would not have been compromised.

98. As a result of Dropbox's above-described wrongful actions, inaction, and want of ordinary care that directly and proximately caused the Data Breach, Plaintiff and all other Class Members have suffered, and will continue to suffer, economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well- established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach, including the increased risks of identity theft they face and will continue to face; and (vii) actual or attempted fraud.

COUNT II

NEGLIGENCE PER SE

(On Behalf of Plaintiff and the Nationwide Class)

99. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

100. Dropbox's duties arise from Section 5 of the FTC Act ("**FTCA**"), 15 U.S.C. § 45(a)(1), which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, the unfair act or practice by a business, such as Dropbox, of failing to employ reasonable measures to protect and secure PII.

101. Dropbox violated Security Rules and Section 5 of the FTCA by failing to use reasonable measures to protect Plaintiff's and all other Class Members' PII and not complying with applicable industry standards. Dropbox's conduct was particularly unreasonable given the nature and amount of PII it obtains and stores, and the foreseeable consequences of a data breach involving PII including, specifically, the substantial damages that would result to Plaintiff and the other Class Members.

102. Dropbox's violations of Security Rules and Section 5 of the FTCA constitutes negligence per se.

103. Plaintiff and Class Members are within the class of persons that Security Rules and Section 5 of the FTCA were intended to protect.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

104. The harm occurring because of the Data Breach is the type of harm Security Rules and Section 5 of the FTCA were intended to guard against.

105. It was reasonably foreseeable to Dropbox that its failure to exercise reasonable care in safeguarding and protecting Plaintiff's and Class Members' PII by failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems, would result in the release, disclosure, and dissemination of Plaintiff's and Class Members' PII to unauthorized individuals.

106. The injury and harm that Plaintiff and the other Class Members suffered was the direct and proximate result of Dropbox's violations of Security Rules and Section 5 of the FTCA. Plaintiff and Class Members have suffered (and will continue to suffer) economic damages and other injury and actual harm in the form of, inter alia: (i) a substantially increased risk of identity theft—risks justifying expenditures for protective and remedial services for which they are entitled to compensation; (ii) improper disclosure of their PII; (iii) breach of the confidentiality of their PII; (iv) deprivation of the value of their PII, for which there is a well-established national and international market; (v) lost time and money incurred to mitigate and remediate the effects of the Data Breach; and (vi) actual or attempted fraud.

COUNT III

BREACH OF FIDUCIARY DUTY

(On Behalf of Plaintiff and the Nationwide Class)

107. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein.

108. Plaintiff and Class Members either directly or indirectly gave Dropbox their PII in confidence, believing that Dropbox would protect that information. Plaintiff and Class Members would not have provided Dropbox with this information had they known it would not be adequately protected. Dropbox's acceptance and storage of Plaintiff's and Class Members' PII created a fiduciary relationship between Dropbox and Plaintiff and Class Members. Considering this relationship, Dropbox must act

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

primarily for the benefit of its consumers, which includes safeguarding and protecting Plaintiff's and Class Members' PII.

109. Dropbox has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of their relationship. It breached that duty by failing to properly protect the integrity of the system containing Plaintiff's and Class Members' PII, failing to safeguard the PII of Plaintiff and Class Members it collected.

110. As a direct and proximate result of Dropbox's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including, but not limited to: (i) a substantial increase in the likelihood of identity theft; (ii) the compromise, publication, and theft of their PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from unauthorized use of their PIII; (iv) lost opportunity costs associated with effort attempting to mitigate the actual and future consequences of the Data Breach; (v) the continued risk to their PII which remains in Dropbox's possession; (vi) future costs in terms of time, effort, and money that will be required to prevent, detect, and repair the impact of the PII compromised as a result of the Data Breach; and (vii) actual or attempted fraud.

COUNT IV

UNJUST ENRICHMENT

(On Behalf of Plaintiff and the Nationwide Class)

111. Plaintiff realleges and incorporates by reference all preceding paragraphs as if fully set forth herein. This claim is pleaded in the alternative to the implied contract claim pursuant to Fed. R. Civ. P. 8(d).

112. Plaintiff and Class Members conferred a monetary benefit upon Dropbox in the form of monies paid for production services or other services.

113. Dropbox accepted or had knowledge of the benefits conferred upon it by Plaintiff and Class Members. Dropbox also benefitted from the receipt of Plaintiff's and Class Members' PII.

114. As a result of Dropbox's conduct, Plaintiff and Class Members suffered actual damages in an amount equal to the difference in value between their payments made with reasonable data privacy

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

and security practices and procedures that Plaintiff and Class Members paid for, and those payments without reasonable data privacy and security practices and procedures that they received.

115. Dropbox should not be permitted to retain the money belonging to Plaintiff and Class Members because Dropbox failed to adequately implement the data privacy and security procedures for itself that Plaintiff and Class Members paid for and that were otherwise mandated by federal, state, and local laws. and industry standards.

116. Dropbox should be compelled to provide for the benefit of Plaintiff and Class Members all unlawful proceeds received by it because of the conduct and Data Breach alleged herein.

COUNT V

BREACH OF IMPLIED CONTRACT

(On Behalf of Plaintiff and the Nationwide Class)

117. Plaintiff realleges and incorporates by reference all allegations of the preceding factual allegations as though fully set forth herein.

118. Defendant required Plaintiff and Class Members to provide or authorize the transfer of their PII for Dropbox to provide services. In exchange, Dropbox entered implied contracts with Plaintiff and Class Members in which Dropbox agreed to comply with its statutory and common law duties to protect Plaintiff's and Class Members' PII and to timely notify them in the event of a data breach.

119. Plaintiff and Class Members would not have provided their PII to Dropbox had they known that Dropbox would not safeguard their PII, as promised, or provide timely notice of a data breach.

120. Plaintiff and Class Members fully performed their obligations under their implied contracts with Dropbox.

121. Defendant breached the implied contracts by failing to safeguard Plaintiff's and Class Members' PII and by failing to provide them with timely and accurate notice of the Data Breach.

122. The losses and damages Plaintiff and Class Members sustained (as described above) were the direct and proximate result of Dropbox's breach of its implied contracts with Plaintiff and Class Members.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

COUNT VI

VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT OF 2018 Cal. Civ. Code §§ 1798.100 et seq. ("CCPA")

(On Behalf of Plaintiff Aquelia Walker and the California Subclass)

123. Plaintiff realleges and incorporates all previous allegations as though fully set forth herein.

124. As more personal information about consumers is collected by businesses, consumers' ability to properly protect and safeguard their privacy has decreased. Consumers entrust businesses with their personal information on the understanding that businesses will adequately protect it from unauthorized access.

125. As a result, in 2018, the California Legislature passed the CCPA, giving consumers broad protections and rights intended to safeguard their personal information. Among other things, the CCPA imposes an affirmative duty on certain businesses that maintain personal information about California residents to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the information collected.

126. Dropbox is subject to the CCPA and failed to implement such procedures which resulted in the Data Breach.

127. Section 1798.150(a)(1) of the CCPA provides: "Any consumer whose nonencrypted or nonredacted personal information, as defined [by the CCPA] is subject to an unauthorized access and exfiltration, theft, or disclosure because of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for" statutory or actual damages, injunctive or declaratory relief, and any other relief the court deems proper.

128. Plaintiff is a "consumer" as defined by Civ. Code § 1798.140(g) because he is natural person residing in the state of California.

129. Dropbox is a "business" as defined by Civ. Code § 1798.140(c).

130. The CCPA provides that "personal information" includes "[a]n individual's first name or first initial and the individual's last name in combination with any one or more of the following data

elements, when either the name or the data elements are not encrypted or redacted . . . (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account." See Civ. Code § 1798.150(a)(1); Civ. Code § 1798.81.5(d)(1)(A).

131. Plaintiff's Private Information compromised in the Data Breach constitutes "personal information" within the meaning of the CCPA.

132. Through the Data Breach, Plaintiff's private information was accessed without authorization, exfiltrated, and stolen by criminals in a nonencrypted and/or nonredacted format.

133. The Data Breach occurred because of Dropbox's failure to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

134. Simultaneously herewith, Plaintiff is providing notice to Defendant pursuant to Cal. Civ. Code § 1798.150(b)(1), identifying the specific provisions of the CCPA. Plaintiff alleges Dropbox has violated or is violating. Although a cure is not possible under the circumstances, if (as expected) Dropbox is unable to cure or does not cure the violation within 30 days, Plaintiff will amend this Complaint to pursue actual or statutory damages as permitted by Cal. Civ. Code § 1798.150(a)(1)(A).

135. As a result of Dropbox's failure to implement and maintain reasonable security procedures and practices that resulted in the Data Breach, Plaintiff seeks statutory damages of up to $750 per class member (and no less than $100 per class member), actual damages to the extent they exceed statutory damages, injunctive and declaratory relief, and any other relief as deemed appropriate by the Court.

COUNT VII

VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT

Cal. Civ. Code §§ 1750 et seq. ("CLRA")

(On Behalf of Plaintiff Aquelia Walker and the California Subclass)

136. Plaintiff realleges and incorporates by reference every allegation contained elsewhere in this Complaint as if fully set forth herein.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

137. This cause of action is brought pursuant to the California Consumers Legal Remedies Act (the "**CLRA**"), California Civil Code § 1750, et seq. This cause of action does not seek monetary damages currently but is limited solely to injunctive relief. Plaintiff will later amend this Complaint to seek damages in accordance with the CLRA after providing Defendant with notice required by California Civil Code § 1782.

138. Plaintiff and Class Members are "consumers," as the term is defined by California Civil Code § 1761(d).

139. Plaintiff, Class Members and Defendant have engaged in "transactions," as that term is defined by California Civil Code § 1761(e).

140. 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.

141. 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."

142. Defendant violated this provision by representing that Defendant took appropriate measures to protect Plaintiff's and the Class Members' PII. Additionally, Defendant improperly handled, stored, or protected either unencrypted or partially encrypted data.

143. As a result, Plaintiff and the Class Members were induced to provide their PII to Defendant.

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

145. Pursuant to Civil Code § 1780(a)(2) and (a)(5), Plaintiff seeks 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 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

146. Plaintiff and the Class Members suffered injuries caused by Defendant's misrepresentations, because they provided their PII believing that Defendant would adequately protect this information.

147. Plaintiff and Class Members may be irreparably harmed and/or denied an effective and complete remedy if such an order is not granted.

148. The unfair and deceptive acts and practices of Defendant, as described above, present a serious threat to Plaintiff and members of the Class.

COUNT VIII

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW Cal. Bus. and Prof. Code §§ 17200, et seq. ("UCL")

(On Behalf of Plaintiff Aquelia Walker and the California Subclass)

149. Plaintiff re-alleges and incorporates by reference all preceding factual allegations as though fully set forth herein.

150. Plaintiff brings this claim on behalf of themselves and the Class.

151. The California Unfair Competition Law, Cal. Bus. & Prof. Code §17200, et seq. ("**UCL**"), prohibits any "unlawful," "fraudulent" or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

152. By reason of Dropbox's above-described wrongful actions, inaction, and omission, the resulting Data Breach, and the unauthorized disclosure of Plaintiff's and Class members' PII, Defendant engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

153. Dropbox's business practices as alleged herein are unfair because they offend established public policy and are immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers, in that the private and confidential PII of consumers has been compromised for all to see, use, or otherwise exploit.

154. Dropbox's practices were unlawful and in violation of the CCPA and CLRA and Dropbox's own privacy policy because Dropbox failed to take reasonable measures to protect Plaintiff's and Class members' PII.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

155. Defendant's business practices as alleged herein are fraudulent because they are likely to deceive consumers into believing that the PII they provide to Dropbox will remain private and secure, when in fact it was not private and secure.

156. Plaintiff and Class Members suffered (and continue to suffer) injury in fact and lost money or property as a direct and proximate result of Dropbox's above-described wrongful actions, inaction, and omissions including, inter alia, the unauthorized release and disclosure of their PII.

157. Dropbox's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff's and Class Members' PII also constitute "unfair" business acts and practices within the meaning of Cal. Bus. & Prof. Code § 17200 et seq., in that Dropbox's conduct was substantially injurious to Plaintiff and Class Members, offensive to public policy, immoral, unethical, oppressive, and unscrupulous, and the gravity of Dropbox's conduct outweighs any alleged benefits attributable to such conduct.

158. But for Dropbox's misrepresentations and omissions, Plaintiff and Class Members would not have provided their PII to Defendant or would have insisted that their PII be more securely protected.

159. As a direct and proximate result of Dropbox's above-described wrongful actions, inaction, and omissions, the resulting Data Breach, and the unauthorized release and disclosure of Plaintiff and Class Members' PII, they have been injured as follows: (1) the loss of the opportunity to control how their PII is used; (2) the diminution in the value and/or use of their PII entrusted to Defendant; (3) the increased, imminent risk of fraud and identity theft; (4) the compromise, publication, and/or theft of their PII; and (5) costs associated with monitoring their PII, amongst other things.

160. Plaintiff takes upon herself enforcement of the laws violated by Dropbox in connection with the reckless and negligent disclosure of PII. There is a financial burden incurred in pursuing this action and it would be against the interests of justice to penalize Plaintiff by forcing her to pay attorneys' fees and costs from the recovery in this action. Therefore, an award of attorneys' fees and costs is appropriate under California Code of Civil Procedure § 1021.5.

///

///

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, pray for judgment as follows:

a. For an Order certifying this action as a class action and appointing Plaintiff and her counsel to represent the Class;

b. For equitable relief enjoining Dropbox from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and Class Members' PII;

c. For equitable relief compelling Dropbox to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of PII compromised during the Data Breach;

d. For an order requiring Dropbox to pay for credit monitoring services for Plaintiff and the Class of a duration to be determined at trial;

e. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

f. For an award of punitive damages, as allowable by law;

g. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

h. Pre- and post-judgment interest on any amounts awarded; and

i. Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: May 2, 2024

CLARKSON LAW FIRM, P.C.

/s/ Yana Hart
Ryan J. Clarkson, Esq.
Yana Hart, Esq.
Tiara Avaness, Esq.
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
rclarkson@clarksonlawfirm.com
yhart@clarksonlawfirm.com
tavaness@clarksonlawfirm.com

STERLINGTON, PLLC
Jennifer Czeisler *(PHV application forthcoming)*
Edward Ciolko *(PHV application forthcoming)*
One World Trade Center
85th Floor
New York, NY 10007
(516) 457-9571
jen.czeisler@sterlingtonlaw.com
edward.ciolko@sterlingtonlaw.com

EVANGELISTA WORLEY LLC
James M. Evangelista *(PHV application forthcoming)*
10 Glenlake Parkway, Suite 130
Atlanta, GA 30328
(404) 205-8400
jim@ewlawllc.com

Attorneys for Plaintiff and the Proposed Classes

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway, Malibu, CA 90265 | P: (213) 788-4050 F: (213) 788-4070 | clarksonlawfirm.com

CIVIL COVER SHEET

The JS-CAND 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 in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

AQUELIA WALKER, on behalf of herself and all others who are similarly situated

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

Yana Hart, Esq. - Clarkson Law Firm, P.C. - 22525 Pacific Coast Highway Malibu, CA 90265
(213) 788-4050, yhart@clarksonlawfirm.com

DEFENDANTS

DROPBOX, INC.

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
- ☐ 2 U.S. Government Defendant
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☒ 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)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 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 & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 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:
Data Breach/Privacy Class Action

VII. REQUESTED IN COMPLAINT:

✓ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $ 5,000,000.00

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

VIII. RELATED CASE(S), IF ANY *(See instructions):*

JUDGE

DOCKET NUMBER

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 05/02/2024

SIGNATURE OF ATTORNEY OF RECORD /s/ Yana Hart, Esq.

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 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 in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate 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 Federal Rule of Civil Procedure 8(a), 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.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 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.

(4) Diversity of citizenship. This refers to suits under 28 USC § 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-CAND 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 the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

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 Federal Rule of Civil Procedure 23.

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-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

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