

CLARKSON LAW FIRM, P.C.

Ryan J. Clarkson (SBN 257074)

rclarkson@clarksonlawfirm.com

Yana Hart (SBN 306499)

yhart@clarksonlawfirm.com

Tiara Avanes (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

1 **CLASS ACTION COMPLAINT**

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

7 **NATURE OF THE ACTION**

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

13 2. This class action arises out of the recent targeted cyberattack against Dropbox that enabled
14 a third party to access Defendant’s computer systems and data, resulting in the compromise of highly
15 sensitive PII (the “**Data Breach**”).²

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

20 _____
21 ¹ DropBox Sign Team, *A Recent Security Incident Involving Dropbox Sign*, DROPBOX SIGN (May 1,
22 2024), <https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign> (Last accessed
23 May 2, 2024).

24 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),
25 <https://thehackernews.com/2024/05/dropbox-discloses-breach-of-digital.html>; Eduard Kovacs,
26 *Hackers Compromised Dropbox eSignature Service*, SECURITYWEEK (May 2, 2024),
<https://www.securityweek.com/dropbox-data-breach-impacts-customer-information/>. (Last accessed
27 May 2, 2024)

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

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

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

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

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

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

25 ³ DropBox Sign Team, *A Recent Security Incident Involving Dropbox Sign*, DROPBOX SIGN (May 1,
26 2024), <https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign> (Last accessed
27 May 2, 2024).

28 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).

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

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

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

13 12. As a result of Dropbox’s inadequate security and breach of its duties and obligations, the
14 PII of Plaintiff and Class Members was compromised through disclosure to an unauthorized criminal
15 third party. Plaintiff and Class Members have suffered injuries as a direct and proximate result of
16 Defendant’s conduct. These injuries include: (i) diminution in value and/or lost value of PII, a form of
17 property that Dropbox obtained from Plaintiff and Class Members; (ii) out-of-pocket expenses
18 associated with preventing, detecting, and remediating identity theft, social engineering, and other
19 unauthorized use of their PII; (iii) opportunity costs associated with attempting to mitigate the actual
20 consequences of the Data Breach, including but not limited to lost time; (iv) the continued, long term,
21 and certain increased risk that unauthorized persons will access and abuse Plaintiff’s and Class
22 Members’ PII; (v) the continued and certain increased risk that the PII that remains in Defendant’s
23 possession is subject to further unauthorized disclosure for so long as Defendant fails to undertake
24 proper measures to protect the PII; (v) invasion of privacy and increased risk of fraud and identity theft;
25 and (vi) theft of their PII and the resulting loss of privacy rights in that information. This action seeks
26 to remedy these failings and their consequences. Plaintiff and Class Members have a continuing interest
27
28

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

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

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

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

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

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

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

27 ///

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

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

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

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

17 23. Plaintiff, on behalf of herself and all other Class Members, brings claims for negligence,
18 negligence per se, breach of implied contract, breach of fiduciary duty, unjust enrichment, and for
19 declaratory and injunctive relief. To remedy these violations of law, Plaintiff and Class Members thus
20 seek actual damages, statutory damages, restitution, and injunctive and declaratory relief (including
21 significant improvements to Dropbox's data security protocols and employee training practices),
22 reasonable attorneys' fees, costs, and expenses incurred in bringing this action, and all other remedies
23 this Court deems just and proper.

24 ///

25 ///

26 ///

27 ///

28

JURISDICTION AND VENUE

1
2 24. This Court has subject matter jurisdiction over this action pursuant to the Class Action
3 Fairness Act of 2005, 28 U.S.C. § 1332(d)(2), because: (i) the amount in controversy exceeds \$5 million,
4 exclusive of interest and costs; (ii) the number of class members exceeds 100 and (iii) minimal diversity
5 exists because many class members, including Plaintiff has different citizenship from Defendant.

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

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

PARTIES

Plaintiff Aquelia Walker

17
18 27. Plaintiff Aquelia Walker (“**Plaintiff**”) is a citizen of the State of California. At all relevant
19 times, Plaintiff has resided in Clovis, California.

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

26 29. On May 1, 2024, Plaintiff received notice of the Data Breach via email. Deeply concerned
27 and troubled, Plaintiff immediately went to the internet to investigate the Data Breach because Plaintiff
28

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

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

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

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

10 **Defendant Dropbox, Inc.**

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

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

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

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

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

24 ///

25 ///

26 _____
27 ⁷ GlobalData, *Dropbox Inc: Company Profile*, GLOBALDATA, N.D.,
28 <https://www.globaldata.com/company-profile/dropbox-inc/>. (Last accessed May 2, 2024).

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)

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

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

8 42. Additionally, Plaintiff and Class Members’ account authentication information, such as
 9 “API keys, OAuth tokens, and multi-factor authentication,”¹⁴ was compromised. With this information,
 10 the threat actor had access to users’ accounts, which stored sensitive documents and agreements, as well
 11 as payment information.

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

17 44. PII is a valuable property right.¹⁶ “Firms are now able to attain significant market
 18 valuations by employing business models predicated on the successful use of personal data within the
 19
 20

21 ¹² *Id.*

22 ¹³ *Id.*

23 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>.

24 ¹⁵ Dropbox, Inc., *Dropbox Sign*, DROPBOX, N.D., <https://www.dropbox.com/sign>. (Last accessed May
 25 2, 2024)

26 ¹⁶ See Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND
 27 COMMUNICATION TECHNOLOGY 26 (May 2015),
https://www.researchgate.net/publication/283668023_The_Value_of_Personal_Data (“The value of
 28 [personal] information is well understood by marketers who try to collect as much data about personal
 conducts and preferences as possible...”).

1 existing legal and regulatory frameworks.”¹⁷ It is estimated that American companies have spent over
 2 \$19 billion on acquiring personal data of consumers in 2018.¹⁸ It is so valuable to identity thieves that
 3 once PII has been disclosed, criminals often trade it on the “cyber black-market,” or the “dark web,” for
 4 many years.

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

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

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

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

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

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

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

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

26 ¹⁸ U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use Solutions in
 27 2018, Up 17.5% from 2017, INTERACTIVE ADVERTISING BUREAU (Dec. 5, 2018),
 28 <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.*

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

3 **B. Dropbox Failed to Comply with FTC Guidelines**

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

9 52. The FTC has promulgated numerous guides for businesses which highlight the importance
10 of implementing reasonable data security practices. According to the FTC, the need for data security
11 should be factored into all business decision-making.

12 53. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for*
13 *Business*, which established cyber-security guidelines for businesses. The guidelines note that
14 businesses should protect the personal customer information that they keep; properly dispose of personal
15 information that is no longer needed; encrypt information stored on computer networks; understand
16 their network’s vulnerabilities; and implement policies to correct any security problems.²¹ The
17 guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon
18 as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the
19 system; watch for large amounts of data being transmitted from the system; and have a response plan
20 ready in the event of a breach.²²

21 54. The FTC further recommends that companies not maintain PII longer than is needed for
22 authorization of a transaction; limit access to sensitive data; require complex passwords to be used on
23 networks; use industry-tested methods for security; monitor for suspicious activity on the network; and
24 verify that third-party service providers have implemented reasonable security measures.

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

²² *Id.*

1 55. The FTC has brought enforcement actions against businesses for failing to adequately and
2 reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to
3 protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited
4 by Section 5 of the Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from
5 these actions further clarify the measures businesses must take to meet their data security obligations.

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

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

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

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

19 60. Dropbox is no stranger to data breaches, as its lax security practices have resulted in
20 multiple disclosures of consumers’ sensitive personal information. In 2011, just three years after it was
21 founded, Dropbox’s systems experienced a bug that would allow anyone to access any account with just
22 the username or email.²³ In 2012, Dropbox accounts were subject to unauthorized access with stolen
23 usernames and passwords, which resulted in attackers gaining access to Dropbox systems.²⁴ **Only four**
24 **years later**, in 2016, did the public learn that approximately 68 million users had been compromised in
25

26 ²³ Fergus O’Sullivan, *A Timeline of Dropbox Security Issues*, PROTON BLOG (January 26, 2024),
27 <https://proton.me/blog/dropbox-security-issues>. (Last accessed, May 2, 2024).

28 ²⁴ *Id.*

1 the 2012 Dropbox incident, making it the “biggest hack in cloud storage history.”²⁵ Recently, in 2022,
2 Dropbox employee credentials were stolen during a phishing attack.²⁶

3 **C. Plaintiff and the Class Have Suffered Injury as a Result of Dropbox’s Data**
4 **Mismanagement**

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

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

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

17 64. PII is a valuable property right.²⁷ The value of PII as a commodity is measurable. “Firms
18 are now able to attain significant market valuations by employing business models predicated on the
19 successful use of personal data within the existing legal and regulatory frameworks.”²⁸ American
20 companies are estimated to have spent over \$19 billion on acquiring personal data of consumers in
21

22 ²⁵ *Id.*

23 ²⁶ *Id.*

24 ²⁷ See, Marc van Lieshout, *The Value of Personal Data*, 457 IFIP ADVANCES IN INFORMATION AND
25 COMMUNICATION TECHNOLOGY (May 2015), <https://www.researchgate.net/publication/283668023>
26 (“The value of [personal] information is well understood by marketers who try to collect as much
27 data about personal conducts and preferences as possible...”). (Last accessed May 2, 2024).

28 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).

1 2018.²⁹ It is so valuable to identity thieves that once PII has been disclosed, criminals often trade it on
2 the “cyber black-market,” or the “dark web,” for many years.

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

8 66. Personal information can be sold at a price ranging from \$40 to \$200, and bank details
9 have a price range of \$50 to \$200.³⁰ Experian reports that a stolen credit or debit card number can sell
10 for \$5 to \$110 on the dark web. Criminals can also purchase access to entire company data breaches
11 from \$900 to \$4,500.³¹

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

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

19
20 ²⁹ *U.S. Firms to Spend Nearly \$19.2 Billion on Third-Party Audience Data and Data-Use*
21 *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).

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

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

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

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

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

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

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

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

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

25
26 _____
27 ³³ Ben Kochman, *FBI, Secret Service Warn of Targeted Ransomware*, LAW360 (Nov. 18, 2019),
28 accessible at <https://www.law360.com/articles/1220974> (Last accessed May 2, 2024).

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

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

- 6 a. Whether Dropbox unlawfully used, maintained, lost, or disclosed Plaintiff's and Class
7 Members' PII;
- 8 b. Whether Dropbox failed to implement and maintain reasonable security procedures and
9 practices appropriate to the nature and scope of the information compromised in the Data
10 Breach;
- 11 c. Whether Dropbox's data security systems prior to and during the Data Breach complied
12 with applicable data security laws and regulations;
- 13 d. Whether Dropbox's data security systems prior to and during the Data Breach were
14 consistent with industry standards;
- 15 e. Whether Dropbox owed a duty to Class Members to safeguard their PII;
- 16 f. Whether Dropbox was subject to (and breached) the FTC Act, the California
17 Confidentiality of Medical Information Act and/or the CCPA;
- 18 g. Whether Dropbox breached its duty to Class Members to safeguard their PII;
- 19 h. Whether computer hackers obtained Class Members' PII in the Data Breach;
- 20 i. Whether Dropbox knew or should have known that its data security systems and
21 monitoring processes were deficient;
- 22 j. Whether Dropbox's conduct was negligent;
- 23 k. Whether Dropbox's acts breaching an implied contract they formed with Plaintiff and the
24 Class Members;
- 25 l. Whether Dropbox was unjustly enriched to the detriment of Plaintiff and the Class;
- 26 m. Whether Dropbox failed to provide notice of the Data Breach in a timely manner; and

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

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

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

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

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

25 ///

26 ///

27 ///

28

CALIFORNIA LAW SHOULD BE APPLIED TO THE NATIONWIDE CLASS

1
2 88. The State of California has a significant interest in regulating the conduct of businesses
3 operating within its borders. California seeks to protect the rights and interests of all California residents
4 and citizens of the United States against a company headquartered and doing business in California.
5 California has a greater interest in the nationwide claims of Plaintiff and members of the Class than any
6 other state and is most intimately concerned with the claims and outcome of this litigation. *See Ehret v.*
7 *Uber Techs., Inc.*, 68 F.Supp.3d 1121, 1130 (N.D. Cal. 2014) (noting courts including the California
8 Supreme Court have permitted the application of California law in cases where alleged
9 misrepresentations were “disseminated from California”); *In re Toyota Motor Corp.*, 785 F.Supp.2d
10 883, 917 (C.D. Cal. 2011) (To determine whether California law should apply, “courts consider where
11 the defendant does business, whether the defendant’s principal offices are located in California, where
12 class members are located, and the location from which advertising and other promotional literature
13 decisions were made.”).

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

25 90. Defendant’s decision to conduct substantial business in California and avail itself of
26 California’s laws, renders the application of California law to the claims herein constitutionally
27 permissible.
28

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.

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

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

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

16 **COUNT IV**

17 **UNJUST ENRICHMENT**

18 ***(On Behalf of Plaintiff and the Nationwide Class)***

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

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

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

26 114. As a result of Dropbox's conduct, Plaintiff and Class Members suffered actual damages
27 in an amount equal to the difference in value between their payments made with reasonable data privacy
28

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

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

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

9 **COUNT V**

10 **BREACH OF IMPLIED CONTRACT**

11 ***(On Behalf of Plaintiff and the Nationwide Class)***

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

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

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

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

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

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

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

1 elements, when either the name or the data elements are not encrypted or redacted . . . (iii) Account
 2 number or credit or debit card number, in combination with any required security code, access code, or
 3 password that would permit access to an individual’s financial account.” See Civ. Code §
 4 1798.150(a)(1); Civ. Code § 1798.81.5(d)(1)(A).

5 131. Plaintiff’s Private Information compromised in the Data Breach constitutes “personal
 6 information” within the meaning of the CCPA.

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

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

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

16 135. As a result of Dropbox’s failure to implement and maintain reasonable security
 17 procedures and practices that resulted in the Data Breach, Plaintiff seeks statutory damages of up to
 18 \$750 per class member (and no less than \$100 per class member), actual damages to the extent they
 19 exceed statutory damages, injunctive and declaratory relief, and any other relief as deemed appropriate
 20 by the Court.

21 COUNT VII

22 VIOLATION OF THE CALIFORNIA CONSUMER LEGAL REMEDIES ACT

23 Cal. Civ. Code §§ 1750 et seq. (“CLRA”)

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

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

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

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

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

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

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

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

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

21 144. As a result of engaging in such conduct, Defendant have violated Civil Code §
22 1770.

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

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

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

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

8 **COUNT VIII**

9 **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW Cal. Bus. and Prof.**

10 **Code §§ 17200, et seq. (“UCL”)**

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

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

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

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

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

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

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

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

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

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

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

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

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

26 ///

27 ///

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.

1 Dated: May 2, 2024

CLARKSON LAW FIRM, P.C.

2 /s/ Yana Hart

3 Ryan J. Clarkson, Esq.

4 Yana Hart, Esq.

5 Tiara Avanness, Esq.

6 22525 Pacific Coast Highway

7 Malibu, CA 90265

8 Tel: (213) 788-4050

9 rclarkson@clarksonlawfirm.com

10 yhart@clarksonlawfirm.com

11 tavaness@clarksonlawfirm.com

STERLINGTON, PLLC

12 Jennifer Czeisler (*PHV application forthcoming*)

13 Edward Ciolko (*PHV application forthcoming*)

14 One World Trade Center

15 85th Floor

16 New York, NY 10007

17 (516) 457-9571

18 jen.czeisler@sterlingtonlaw.com

19 edward.ciolko@sterlingtonlaw.com

EVANGELISTA WORLEY LLC

20 James M. Evangelista (*PHV application forthcoming*)

21 10 Glenlake Parkway, Suite 130

22 Atlanta, GA 30328

23 (404) 205-8400

24 jim@ewlawllc.com

25 *Attorneys for Plaintiff and the Proposed Classes*