

1 Scott Edward Cole, Esq. (S.B. #160744)
Laura Grace Van Note, Esq. (S.B. #310160)
2 Elizabeth Ruth Klos, Esq. (S.B. #346781)
COLE & VAN NOTE
3 555 12th Street, Suite 2100
Oakland, California 94607
4 Telephone: (510) 891-9800
Facsimile: (510) 891-7030
5 Email: sec@colevannote.com
Email: lvn@colevannote.com
6 Email: erk@colevannote.com

7 Attorneys for Representative Plaintiff
and the Plaintiff Class

8
9 **UNITED STATES DISTRICT COURT**
10 **NORTHERN DISTRICT OF CALIFORNIA**

12 SHYRAH STRICKLAND, individually,
and on behalf of all others similarly
13 situated,

14 Plaintiff,

15 v.

16 DROPBOX, INC.,

17 Defendant.

Case No.

CLASS ACTION

COMPLAINT FOR DAMAGES

1. **NEGLIGENCE;**
2. **BREACH OF IMPLIED CONTRACT;**
3. **BREACH OF THE IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING; AND**
4. **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW CAL. BUS. & PROF. CODE §§ 17200, ET SEQ.**

[JURY TRIAL DEMANDED]

22
23 **INTRODUCTION**

24 1. Representative Shyrah Strickland (“Representative Plaintiff”) brings this class
25 action against Dropbox, Inc. (“Defendant”) for its failure to properly secure and safeguard
26 Representative Plaintiff’s and/or Class Members’ personally identifiable information stored within
27 Defendant’s information network, including without limitation, emails, usernames, phone
28 numbers and hashed passwords, in addition to general account settings and certain authentication

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 information such as API Keys, OAuth tokens, and multi-factor authentication (these types of
2 information, *inter alia*, being thereafter referred to as “personally identifiable information” or
3 “PII”).¹ All such information is referred to in the aggregate herein as “Private Information.”

4 2. With this action, Representative Plaintiff seeks to hold Defendant responsible for
5 the harms it caused and will continue to cause Representative Plaintiff and numerous other
6 similarly situated persons in the massive and preventable cyberattack purportedly discovered by
7 Defendant on April 24, 2024, by which cybercriminals infiltrated Defendant’s inadequately
8 protected network and accessed the Private Information which was being kept under-protected (the
9 “Data Breach”).

10 3. While Defendant claims to have discovered the breach as early as April 24, 2024,
11 Defendant failed to inform victims when or for how long the Data Breach occurred. Indeed,
12 Defendant has yet to notify Representative Plaintiff that her information was compromised. On
13 May 3, 2024, Representative Plaintiff received electronic messages from a third party,
14 FundThrough, Inc. informing her that her information may have been exposed in the Data Breach.
15 The Notice received by Representative Plaintiff was dated May 3, 2024.

16 4. Defendant acquired, collected and stored Representative Plaintiff’s and Class
17 Members’ Private Information. Therefore, at all relevant times, Defendant knew or should have
18 known that Representative Plaintiff and Class Members would use Defendant’s services to store
19 and/or share sensitive data, including highly confidential Private Information.

20 5. Defendant disregarded the rights of Representative Plaintiff and Class Members by
21 intentionally, willfully, recklessly and/or negligently failing to take and implement adequate and
22 reasonable measures to ensure that Representative Plaintiff’s and Class Members’ Private
23 Information was safeguarded, failing to take available steps to prevent an unauthorized disclosure
24 of data, and failing to follow applicable, required and appropriate protocols, policies and

25
26 ¹ Personally identifiable information (“PII”) generally incorporates information that can be
27 used to distinguish or trace an individual’s identity, either alone or when combined with other
28 personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information
that on its face expressly identifies an individual. PII also is generally defined to include certain
identifiers that do not on its face name an individual, but that are considered to be particularly
sensitive and/or valuable if in the wrong hands (for example, Social Security numbers, passport
numbers, driver’s license numbers, financial account numbers, etc.).

1 procedures regarding the encryption of data, even for internal use. As a result, Representative
2 Plaintiff's and Class Members' Private Information was compromised through disclosure to an
3 unknown and unauthorized third party—an undoubtedly nefarious third party seeking to profit off
4 this disclosure by defrauding Representative Plaintiff and Class Members in the future.
5 Representative Plaintiff and Class Members have a continuing interest in ensuring their
6 information is and remains safe and are entitled to injunctive and other equitable relief.

7
8 **JURISDICTION AND VENUE**

9 6. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction).
10 Specifically, this Court has subject matter and diversity jurisdiction over this action under 28
11 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum
12 or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the
13 proposed class and at least one other Class Member is a citizen of a state different from Defendant.

14 7. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in
15 this Court under 28 U.S.C. § 1367.

16 8. Defendant is headquartered and routinely conducts business in the State where this
17 District is located, has sufficient minimum contacts in this State and has intentionally availed itself
18 of this jurisdiction by marketing and selling products and services, and by accepting and processing
19 payments for those products and services within this State.

20 9. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of
21 the events that gave rise to Representative Plaintiff's claims took place within this District, and
22 Defendant does business in this Judicial District.

23
24 **PLAINTIFF**

25 10. Representative Plaintiff is an adult individual and, at all relevant times herein, was
26 a resident and citizen of the State of North Carolina. Representative Plaintiff is a victim of the Data
27 Breach.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 11. Defendant received highly sensitive Private Information from Representative
2 Plaintiff in connection with the services Representative Plaintiff received. As a result,
3 Representative Plaintiff's information was among the data accessed by an unauthorized third party
4 in the Data Breach.

5 12. At all times herein relevant, Representative Plaintiff is and was a member of the
6 Class.

7 13. As required in order to obtain services from Defendant, Representative Plaintiff
8 provided Defendant with highly sensitive Private Information.

9 14. Representative Plaintiff's Private Information was exposed in the Data Breach
10 because Defendant stored and/or shared Representative Plaintiff's Private Information.
11 Representative Plaintiff's Private Information was within the possession and control of Defendant
12 at the time of the Data Breach.

13 15. Representative Plaintiff received a letter from Defendant stating Representative
14 Plaintiff's Private Information was involved in the Data Breach (the "Notice").

15 16. As a result, Representative Plaintiff spent time dealing with the consequences of
16 the Data Breach, which included and continues to include, time spent verifying the legitimacy and
17 impact of the Data Breach, exploring credit monitoring and identity theft insurance options, self-
18 monitoring Representative Plaintiff's accounts and seeking legal counsel regarding Representative
19 Plaintiff's options for remedying and/or mitigating the effects of the Data Breach. This time has
20 been lost forever and cannot be recaptured.

21 17. Representative Plaintiff suffered actual injury in the form of damages to and
22 diminution in the value of Representative Plaintiff's Private Information—a form of intangible
23 property that Representative Plaintiff entrusted to Defendant, which was compromised in and as a
24 result of the Data Breach.

25 18. Representative Plaintiff suffered lost time, annoyance, interference and
26 inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss
27 of privacy, as well as anxiety over the impact of cybercriminals accessing, using and selling
28 Representative Plaintiff's Private Information.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 19. Representative Plaintiff suffered imminent and impending injury arising from the
2 substantially increased risk of fraud, identity theft and misuse resulting from Representative
3 Plaintiff's Private Information being placed in the hands of unauthorized third parties/criminals.

4 20. Representative Plaintiff has a continuing interest in ensuring that Representative
5 Plaintiff's Private Information, which, upon information and belief, remains backed up in
6 Defendant's possession, is protected and safeguarded from future breaches.

7
8 **DEFENDANT**

9 21. Defendant is a Delaware corporation headquartered in California with its principal
10 executive office located at 1800 Owens Street, Suite 200, San Francisco, California 94518.
11 Defendant is a cloud storage solution, equipped with features allowing users to store files,
12 documents, and photos online and then access them from any device.²³

13 22. The true names and capacities of persons or entities, whether individual, corporate,
14 associate or otherwise, who may be responsible for some of the claims alleged here are currently
15 unknown to Representative Plaintiff. Representative Plaintiff will seek leave of court to amend
16 this Complaint to reflect the true names and capacities of such responsible parties when their
17 identities become known.

18
19 **CLASS ACTION ALLEGATIONS**

20 23. Representative Plaintiff brings this action pursuant to the provisions of Rules 23(a),
21 (b)(2), and (b)(3) of the Federal Rules of Civil Procedure, on behalf of Representative Plaintiff and
22 the following class (collectively, the "Class"):

23 **Plaintiff Class:**

24 "All individuals within the United States of America whose Private
25 Information was exposed to unauthorized third parties as a result of the data
26 breach allegedly discovered by Defendant on April 24, 2024."

27 ² "What is Dropbox?" *Dropbox*,
28 <https://www.dropbox.com/features#:~:text=Dropbox%20is%20a%20cloud%20storage,access%20them%20from%20any%20device/> (Last accessed May 7, 2024).

COLE & VAN NOTE
 ATTORNEYS AT LAW
 555 12TH STREET, SUITE 2100
 OAKLAND, CA 94607
 TEL: (510) 891-9800

1 24. Excluded from the Class are the following individuals and/or entities: Defendant
 2 and Defendant’s parents, subsidiaries, affiliates, officers and directors and any entity in which
 3 Defendant has a controlling interest, all individuals who make a timely election to be excluded
 4 from this proceeding using the correct protocol for opting out, any and all federal, state or local
 5 governments, including but not limited to its departments, agencies, divisions, bureaus, boards,
 6 sections, groups, counsel and/or subdivisions, and all judges assigned to hear any aspect of this
 7 litigation, as well as their immediate family members.

8 25. In the alternative, Representative Plaintiff may request additional subclasses as
 9 necessary based, e.g., on the types of Private Information that were compromised.

10 26. Representative Plaintiff reserves the right to amend the above definition or to
 11 propose subclasses in subsequent pleadings and its motion for class certification.

12 27. This action has been brought and may properly be maintained as a class action
 13 under Federal Rules of Civil Procedure Rule 23 because there is a well-defined community of
 14 interest in the litigation and membership in the proposed Class is easily ascertainable.

15 a. Numerosity: A class action is the only available method for the fair and
 16 efficient adjudication of this controversy. The members of the Plaintiff
 17 Class are so numerous that joinder of all members is impractical, if not
 impossible. Membership in the Class will be determined by analysis of
 Defendant’s records.

18 b. Commonality: Representative Plaintiff and Class Members share a
 19 community of interest in that there are numerous common questions and
 20 issues of fact and law which predominate over any questions and issues
 solely affecting individual members, including but not necessarily limited
 to:

- 21 1) Whether Defendant had a legal duty to Representative Plaintiff and the
 22 Class to exercise due care in collecting, storing, using and/or
 safeguarding their Private Information;
- 23 2) Whether Defendant knew or should have known of the susceptibility
 24 of its data security systems to a data breach;
- 25 3) Whether Defendant’s security procedures and practices to protect its
 26 systems were reasonable in light of the measures recommended by data
 security experts;
- 27 4) Whether Defendant’s failure to implement adequate data security
 28 measures allowed the Data Breach to occur;

COLE & VAN NOTE
 ATTORNEYS AT LAW
 555 12TH STREET, SUITE 2100
 OAKLAND, CA 94607
 TEL: (510) 891-9800

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- 5) Whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;
 - 6) Whether Defendant adequately, promptly and accurately informed Representative Plaintiff and Class Members that their Private Information had been compromised;
 - 7) How and when Defendant actually learned of the Data Breach;
 - 8) Whether Defendant’s conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the loss of Representative Plaintiff’s and Class Members’ Private Information;
 - 9) Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
 - 10) Whether Defendant engaged in unfair, unlawful or deceptive practices by failing to safeguard Representative Plaintiff’s and Class Members’ Private Information;
 - 11) Whether Representative Plaintiff and Class Members are entitled to actual and/or statutory damages and/or whether injunctive, corrective and/or declaratory relief and/or an accounting is/are appropriate as a result of Defendant’s wrongful conduct; and
 - 12) Whether Representative Plaintiff and Class Members are entitled to restitution as a result of Defendant’s wrongful conduct.
- c. Typicality: Representative Plaintiff’s claims are typical of the claims of the Plaintiff Class. Representative Plaintiff and all members of the Plaintiff Class sustained damages arising out of and caused by Defendant’s common course of conduct in violation of law, as alleged herein.
- d. Adequacy of Representation: Representative Plaintiff in this class action is an adequate representative of the Plaintiff Class in that the Representative Plaintiff has the same interest in the litigation of this case as the Class Members, is committed to vigorous prosecution of this case and has retained competent counsel who are experienced in conducting litigation of this nature. Representative Plaintiff is not subject to any individual defenses unique from those conceivably applicable to other Class Members or the Class in its entirety. Representative Plaintiff anticipates no management difficulties in this litigation.
- e. Superiority of Class Action: Since the damages suffered by individual Class Members, while not inconsequential, may be relatively small, the expense and burden of individual litigation by each member makes or may make it impractical for members of the Plaintiff Class to seek redress individually for the wrongful conduct alleged herein. Should separate actions be brought or be required to be brought by each individual member of the Plaintiff Class, the resulting multiplicity of lawsuits would cause undue hardship and expense for the Court and the litigants. The prosecution of separate actions would also create a risk of inconsistent rulings which might be dispositive of the interests of the Class Members who are not parties to the

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 adjudications and/or may substantially impede their ability to adequately
2 protect their interests.

3 28. Class certification is proper because the questions raised by this Complaint are of
4 common or general interest affecting numerous persons, such that it is impracticable to bring all
5 Class Members before the Court.

6 29. This class action is also appropriate for certification because Defendant has acted
7 or refused to act on grounds generally applicable to Class Members, thereby requiring the Court's
8 imposition of uniform relief to ensure compatible standards of conduct toward the Class Members
9 and making final injunctive relief appropriate with respect to the Class in its entirety. Defendant's
10 policies and practices challenged herein apply to and affect Class Members uniformly and
11 Representative Plaintiff's challenge of these policies and practices hinges on Defendant's conduct
12 with respect to the Class in its entirety, not on facts or law applicable only to Representative
13 Plaintiff.

14 30. Unless a Class-wide injunction is issued, Defendant may continue in its failure to
15 properly secure the Private Information of Class Members, and Defendant may continue to act
16 unlawfully as set forth in this Complaint.

17 31. Further, Defendant has acted or refused to act on grounds generally applicable to
18 the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the
19 Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil
20 Procedure.

21
22 **COMMON FACTUAL ALLEGATIONS**

23 **The Cyberattack**

24 32. In the course of the Data Breach, one or more unauthorized third parties accessed
25 Class Members' Private Information. Representative Plaintiff was among the individuals whose
26 data was accessed in the Data Breach.

27 33. According to the publicly filed documents, Representative Plaintiff states, on
28 information and belief, that numerous persons were affected by the Data Breach.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 34. Representative Plaintiff was provided the information detailed above upon receipt
2 from a communication from a third party, which prompted Representative Plaintiff to review
3 publicly available documents related to the Breach. Representative Plaintiff was not aware of the
4 Data Breach until receiving that communication from the third party.

5
6 **Defendant’s Failed Response to the Breach**

7 35. Upon information and belief, the unauthorized third-party cybercriminals gained
8 access to Representative Plaintiff’s and Class Members’ Private Information with the intent of
9 misusing the Private Information, including marketing and selling Representative Plaintiff’s and
10 Class Members’ Private Information.

11 36. Defendant still has not sent Notice to persons whose Private Information Defendant
12 confirmed was potentially compromised as a result of the Data Breach.

13 37. Publicly available information regarding the Data Breach included, *inter alia*, the
14 claim that Defendant discovered the unauthorized access leading to the Data Breach began as early
15 as April 24, 2024.

16 38. Defendant had and continues to have obligations created by applicable federal and
17 state law as set forth herein, reasonable industry standards, common law and its own assurances
18 and representations to keep Representative Plaintiff’s and Class Members’ Private Information
19 confidential and to protect such Private Information from unauthorized access.

20 39. Representative Plaintiff and Class Members were required to provide their Private
21 Information to Defendant in order to receive services. Thus, Defendant created, collected and
22 stored Representative Plaintiff’s and Class Members’ Private Information with the reasonable
23 expectation and mutual understanding that Defendant would comply with its obligations to keep
24 such information confidential and secure from unauthorized access.

25 40. Despite this, Representative Plaintiff and the Class Members remain, even today,
26 in the dark regarding what particular data was stolen, the particular malware used and what steps
27 are being taken, if any, to secure their Private Information going forward. Representative Plaintiff
28 and Class Members are thus left to speculate as to where their Private Information ended up, who

1 has used it and for what potentially nefarious purposes. Indeed, they are left to further speculate as
 2 to the full impact of the Data Breach and how exactly Defendant intends to enhance its information
 3 security systems and monitoring capabilities so as to prevent further breaches.

4 41. Representative Plaintiff's and Class Members' Private Information may end up for
 5 sale on the dark web, or simply fall into the hands of companies that will use the detailed Private
 6 Information for targeted marketing without Representative Plaintiff's and/or Class Members'
 7 approval. Either way, unauthorized individuals can now easily access Representative Plaintiff's
 8 and Class Members' Private Information.

9
 10 **Defendant Collected/Stored Class Members' Private Information**

11 42. Defendant acquired, collected, stored and assured reasonable security over
 12 Representative Plaintiff's and Class Members' Private Information.

13 43. As a condition of its relationships with Representative Plaintiff and Class Members,
 14 Defendant required that Representative Plaintiff and Class Members entrust Defendant with highly
 15 sensitive and confidential Private Information. Defendant, in turn, stored that information on
 16 Defendant's system that was ultimately affected by the Data Breach.

17 44. By obtaining, collecting and storing Representative Plaintiff's and Class Members'
 18 Private Information, Defendant assumed legal and equitable duties over the Private Information
 19 and knew or should have known that it was thereafter responsible for protecting Representative
 20 Plaintiff's and Class Members' Private Information from unauthorized disclosure.

21 45. Representative Plaintiff and Class Members have taken reasonable steps to
 22 maintain their Private Information's confidentiality. Representative Plaintiff and Class Members
 23 relied on Defendant to keep their Private Information confidential and securely maintained, to use
 24 this information for business purposes only and to make only authorized disclosures of this
 25 information.

26 46. Defendant could have prevented the Data Breach by properly securing and
 27 encrypting and/or more securely encrypting its servers generally, as well as Representative
 28 Plaintiff's and Class Members' Private Information.

1 47. Defendant's negligence in safeguarding Representative Plaintiff's and Class
2 Members' Private Information is exacerbated by repeated warnings and alerts directed to
3 protecting and securing sensitive data, as evidenced by the trending data breach attacks in recent
4 years.

5 48. Due to the high-profile nature of these breaches, and other breaches of its kind,
6 Defendant was and/or certainly should have been on notice and aware of such attacks occurring in
7 its industry and, therefore, should have assumed and adequately performed the duty of preparing
8 for such an imminent attack. This is especially true given that Defendant is a large, sophisticated
9 operation with the resources to put adequate data security protocols in place.

10 49. And yet, despite the prevalence of public announcements of data breach and data
11 security compromises, Defendant failed to take appropriate steps to protect Representative
12 Plaintiff's and Class Members' Private Information from being compromised.

13
14 **Defendant Had an Obligation to Protect the Stolen Information**

15 50. In failing to adequately secure Representative Plaintiff's and Class Member's
16 sensitive data, Defendant breached duties it owed Representative Plaintiff and Class Members
17 under statutory and common law.

18 51. Representative Plaintiff and Class Members surrendered their highly sensitive
19 Private Information to Defendant under the implied condition that Defendant would keep it private
20 and secure. Accordingly, Defendant also has an implied duty to safeguard their Private
21 Information, independent of any statute.

22 52. Defendant was also prohibited by the Federal Trade Commission Act (the "FTC
23 Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting
24 commerce." The Federal Trade Commission (the "FTC") has concluded that a company's failure
25 to maintain reasonable and appropriate data security for consumers' sensitive personal information
26 is an "unfair practice" in violation of the FTC Act. *See, e.g., FTC v. Wyndham Worldwide Corp.*,
27 799 F.3d 236 (3d Cir. 2015).

28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 53. In addition to its obligations under federal and state laws, Defendant owed a duty
2 to Representative Plaintiff and Class Members to exercise reasonable care in obtaining, retaining,
3 securing, safeguarding, deleting and protecting the Private Information in Defendant’s possession
4 from being compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant
5 owed a duty to Representative Plaintiff and Class Members to provide reasonable security,
6 including consistency with industry standards and requirements, and to ensure that its computer
7 systems, networks and protocols adequately protected Representative Plaintiff’s and Class
8 Members’ Private Information.

9 54. Defendant owed a duty to Representative Plaintiff and Class Members to design,
10 maintain and test its computer systems, servers and networks to ensure that all Private Information
11 in its possession was adequately secured and protected.

12 55. Defendant owed a duty to Representative Plaintiff and Class Members to create and
13 implement reasonable data security practices and procedures to protect all Private Information in
14 its possession, including not sharing information with other entities who maintained sub-standard
15 data security systems.

16 56. Defendant owed a duty to Representative Plaintiff and Class Members to
17 implement processes that would immediately detect a breach of its data security systems in a timely
18 manner.

19 57. Defendant owed a duty to Representative Plaintiff and Class Members to act upon
20 data security warnings and alerts in a timely fashion.

21 58. Defendant owed a duty to Representative Plaintiff and Class Members to disclose
22 if its computer systems and data security practices were inadequate to safeguard individuals’
23 Private Information from theft because such an inadequacy would be a material fact in the decision
24 to entrust their Private Information to Defendant.

25 59. Defendant owed a duty of care to Representative Plaintiff and Class Members
26 because they were foreseeable and probable victims of any inadequate data security practices.
27
28

1 60. Defendant owed a duty to Representative Plaintiff and Class Members to encrypt
2 and/or more reliably encrypt Representative Plaintiff's and Class Members' Private Information
3 and monitor user behavior and activity in order to identify possible threats.
4

5 **Value of the Relevant Sensitive Information**

6 61. The high value of Private Information to criminals is evidenced by the prices they
7 will pay for it through the dark web. Numerous sources cite dark web pricing for stolen identity
8 credentials. For example, personal information can be sold at a price ranging from \$40 to \$200,
9 and bank details have a price range of \$50 to \$200.⁴ Experian reports that a stolen credit or debit
10 card number can sell for \$5 to \$110 on the dark web.⁵ Criminals can also purchase access to entire
11 company data breaches from \$999 to \$4,995.⁶

12 62. Between 2005 and 2019, at least 249 million people were affected by healthcare
13 data breaches.⁷ Indeed, during 2019 alone, over 41 million healthcare records were exposed,
14 stolen, or unlawfully disclosed in 505 data breaches.⁸ In short, these sorts of data breaches are
15 increasingly common, especially among healthcare systems, which account for 30.03 percent of
16 overall health data breaches, according to cybersecurity firm Tenable.⁹

17 63. These criminal activities have and will result in devastating financial and personal
18 losses to Representative Plaintiff and Class Members. For example, it is believed that certain
19 Private Information compromised in the 2017 Equifax data breach was being used three years later
20 by identity thieves to apply for COVID-19-related benefits in the state of Oklahoma. Such fraud
21

22
23 ⁴ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct.
16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (Last accessed May 7, 2024).

24 ⁵ *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec.
6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (Last accessed May 7, 2024).

25 ⁶ *In the Dark*, VPNOverview, 2019, available at:
26 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark> (Last accessed May 7, 2024).

27 ⁷ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/>.

28 ⁸ <https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/> (Last accessed May 7, 2024).

⁹ <https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches/> (Last accessed May 7, 2024).

COLE & VAN NOTE
 ATTORNEYS AT LAW
 555 12TH STREET, SUITE 2100
 OAKLAND, CA 94607
 TEL: (510) 891-9800

1 will be an omnipresent threat for Representative Plaintiff and Class Members for the rest of their
 2 lives. They will need to remain constantly vigilant.

3 64. The FTC defines identity theft as “a fraud committed or attempted using the
 4 identifying information of another person without authority.” The FTC describes “identifying
 5 information” as “any name or number that may be used, alone or in conjunction with any other
 6 information, to identify a specific person,” including, among other things, “[n]ame, Social Security
 7 number, date of birth, official State or government issued driver’s license or identification number,
 8 alien registration number, government passport number, employer or taxpayer identification
 9 number.”

10 65. Identity thieves can use Private Information, such as that of Representative Plaintiff
 11 and Class Members which Defendant failed to keep secure, to perpetrate a variety of crimes that
 12 harm victims. For instance, identity thieves may commit various types of government fraud such
 13 as immigration fraud, obtaining a driver’s license or identification card in the victim’s name but
 14 with another’s picture, using the victim’s information to obtain government benefits or filing a
 15 fraudulent tax return using the victim’s information to obtain a fraudulent refund.

16 66. The ramifications of Defendant’s failure to keep secure Representative Plaintiff’s
 17 and Class Members’ Private Information are long lasting and severe. Once Private Information is
 18 stolen, particularly identification numbers, fraudulent use of that information and damage to
 19 victims may continue for years. Indeed, Representative Plaintiff’s and Class Members’ Private
 20 Information was taken by hackers to engage in identity theft or to sell it to other criminals who
 21 will purchase the Private Information for that purpose. The fraudulent activity resulting from the
 22 Data Breach may not come to light for years.

23 67. There may be a time lag between when harm occurs versus when it is discovered
 24 and also between when Private Information is stolen and when it is used. According to the U.S.
 25 Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

26 [L]aw enforcement officials told us that in some cases, stolen data may be held for
 27 up to a year or more before being used to commit identity theft. Further, once stolen
 28 data have been sold or posted on the Web, fraudulent use of that information may

1 continue for years. As a result, studies that attempt to measure the harm resulting
 2 from data breaches cannot necessarily rule out all future harm.¹⁰

3 68. When cybercriminals access financial information, health insurance information
 4 and other personally sensitive data—as they did here—there is no limit to the amount of fraud to
 5 which Defendant may have exposed Representative Plaintiff and Class Members.

6 69. A study by Experian found that the average total cost of medical identity theft is
 7 “about \$20,000” per incident, and that a majority of victims of medical identity theft were forced
 8 to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.¹¹ Almost
 9 half of medical identity theft victims lose their healthcare coverage as a result of the incident, while
 10 nearly one-third saw their insurance premiums rise, and 40 percent were never able to resolve their
 11 identity theft at all.¹²

12 70. And data breaches are preventable.¹³ As Lucy Thompson wrote in the DATA
 13 BREACH AND ENCRYPTION HANDBOOK, “[i]n almost all cases, the data breaches that occurred could
 14 have been prevented by proper planning and the correct design and implementation of appropriate
 15 security solutions.”¹⁴ She added that “[o]rganizations that collect, use, store, and share sensitive
 16 personal data must accept responsibility for protecting the information and ensuring that it is not
 17 compromised....”¹⁵

18 71. Most of the reported data breaches are a result of lax security and the failure to
 19 create or enforce appropriate security policies, rules and procedures. Appropriate information
 20 security controls, including encryption, must be implemented and enforced in a rigorous and
 21 disciplined manner so that a *data breach never occurs*.¹⁶

22 ¹⁰ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at:
 23 <http://www.gao.gov/new.items/d07737.pdf> (Last accessed May 7, 2024).

24 ¹¹ Elinor Mills, “Study: Medical Identity Theft is Costly for Victims,” CNET (Mar, 3, 2010),
 25 <https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/> (Last accessed
 26 May 7, 2024).

27 ¹² *Id.*; see also Healthcare Data Breach: What to Know About them and What to Do After One,
 28 EXPERIAN, <https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/> (Last accessed May 7, 2024).

¹³ Lucy L. Thompson, “Despite the Alarming Trends, Data Breaches Are Preventable,” *in*
 DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).

¹⁴ *Id.* at 17.

¹⁵ *Id.* at 28.

¹⁶ *Id.*

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

- 1 a. to exercise reasonable care in obtaining, retaining, securing, safeguarding,
2 deleting and protecting the Private Information in its possession;
- 3 b. to protect Representative Plaintiff's and Class Members' Private
4 Information using reasonable and adequate security procedures and systems
5 that were/are compliant with industry-standard practices;
- 6 c. to implement processes to quickly detect the Data Breach and to timely act
7 on warnings about data breaches; and
- 8 d. to promptly notify Representative Plaintiff and Class Members of any data
9 breach, security incident or intrusion that affected or may have affected their
10 Private Information.

11 77. Defendant knew that the Private Information was private and confidential and
12 should be protected as private and confidential and, thus, Defendant owed a duty of care not to
13 subject Representative Plaintiff and Class Members to an unreasonable risk of harm because they
14 were foreseeable and probable victims of any inadequate security practices.

15 78. Defendant knew or should have known of the risks inherent in collecting and
16 storing Private Information, the vulnerabilities of its data security systems and the importance of
17 adequate security. Defendant knew about numerous, well-publicized data breaches.

18 79. Defendant knew or should have known that its data systems and networks did not
19 adequately safeguard Representative Plaintiff's and Class Members' Private Information.

20 80. Only Defendant was in the position to ensure that its systems and protocols were
21 sufficient to protect the Private Information that Representative Plaintiff and Class Members had
22 entrusted to it.

23 81. Defendant breached its duties to Representative Plaintiff and Class Members by
24 failing to provide fair, reasonable or adequate computer systems and data security practices to
25 safeguard Representative Plaintiff's and Class Members' Private Information.

26 82. Because Defendant knew that a breach of its systems could damage thousands of
27 individuals, including Representative Plaintiff and Class Members, Defendant had a duty to
28 adequately protect its data systems and the Private Information contained thereon.

83. Representative Plaintiff's and Class Members' willingness to entrust Defendant
with its Private Information was predicated on the understanding that Defendant would take
adequate security precautions. Moreover, only Defendant had the ability to protect its systems and

1 the Private Information it stored on them from attack. Thus, Defendant had a special relationship
2 with Representative Plaintiff and Class Members.

3 84. Defendant also had independent duties under state and federal laws that required
4 Defendant to reasonably safeguard Representative Plaintiff's and Class Members' Private
5 Information and promptly notify them about the Data Breach. These "independent duties" are
6 untethered to any contract between Defendant and Representative Plaintiff and/or the remaining
7 Class Members.

8 85. Defendant breached its general duty of care to Representative Plaintiff and Class
9 Members in, but not necessarily limited to, the following ways:

- 10 a. by failing to provide fair, reasonable or adequate computer systems and data
11 security practices to safeguard Representative Plaintiff's and Class
Members' Private Information;
- 12 b. by failing to timely and accurately disclose that Representative Plaintiff's
13 and Class Members' Private Information had been improperly acquired or
accessed;
- 14 c. by failing to adequately protect and safeguard the Private Information by
15 knowingly disregarding standard information security principles, despite
obvious risks, and by allowing unmonitored and unrestricted access to
16 unsecured Private Information;
- 17 d. by failing to provide adequate supervision and oversight of the Private
18 Information with which it was and is entrusted, in spite of the known risk
and foreseeable likelihood of breach and misuse, which permitted an
19 unknown third party to gather Representative Plaintiff's and Class
Members' Private Information, misuse the Private Information and
intentionally disclose it to others without consent;
- 20 e. by failing to adequately train its employees to not store Private Information
21 longer than absolutely necessary;
- 22 f. by failing to consistently enforce security policies aimed at protecting
23 Representative Plaintiff's and the Class Members' Private Information;
- 24 g. by failing to implement processes to quickly detect data breaches, security
25 incidents or intrusions; and
- 26 h. by failing to encrypt Representative Plaintiff's and Class Members' Private
27 Information and monitor user behavior and activity in order to identify
28 possible threats.

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 86. Defendant's willful failure to abide by these duties was wrongful, reckless and/or
2 grossly negligent in light of the foreseeable risks and known threats.

3 87. As a proximate and foreseeable result of Defendant's grossly negligent conduct,
4 Representative Plaintiff and Class Members have suffered damages and are at imminent risk of
5 additional harm and damages (as alleged above).

6 88. The law further imposes an affirmative duty on Defendant to timely disclose the
7 unauthorized access and theft of the Private Information to Representative Plaintiff and Class
8 Members so that they could and/or still can take appropriate measures to mitigate damages, protect
9 against adverse consequences and thwart future misuse of their Private Information.

10 89. Defendant breached its duty to notify Representative Plaintiff and Class Members
11 of the unauthorized access by failing to notify Representative Plaintiff and Class Members and
12 failing and continuing to fail to provide Representative Plaintiff and Class Members sufficient
13 information regarding the breach. To date, Defendant has not provided sufficient information to
14 Representative Plaintiff and Class Members regarding the extent of the unauthorized access and
15 continues to breach its disclosure obligations to Representative Plaintiff and Class Members.

16 90. Further, through its failure to provide timely and clear notification of the Data
17 Breach to Representative Plaintiff and Class Members, Defendant prevented Representative
18 Plaintiff and Class Members from taking meaningful, proactive steps to, *inter alia*, secure and/or
19 access their Private Information.

20 91. There is a close causal connection between Defendant's failure to implement
21 security measures to protect Representative Plaintiff's and Class Members' Private Information
22 and the harm suffered, or risk of imminent harm suffered, by Representative Plaintiff and Class
23 Members. Representative Plaintiff's and Class Members' Private Information was accessed as the
24 proximate result of Defendant's failure to exercise reasonable care in safeguarding such Private
25 Information by adopting, implementing and maintaining appropriate security measures.

26 92. Defendant's wrongful actions, inactions and omissions constituted (and continue to
27 constitute) common law negligence.
28

1 93. The damages Representative Plaintiff and Class Members have suffered (as alleged
2 above) and will continue to suffer were and are the direct and proximate result of Defendant's
3 grossly negligent conduct.

4 94. Additionally, 15 U.S.C. § 45 (FTC Act, Section 5) prohibits "unfair [...] practices
5 in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or
6 practice by businesses, such as Defendant, of failing to use reasonable measures to protect Private
7 Information. The FTC publications and orders described above also form part of the basis of
8 Defendant's duty in this regard.

9 95. Defendant violated 15 U.S.C. § 45 by failing to use reasonable measures to protect
10 Private Information and not complying with applicable industry standards, as described in detail
11 herein. Defendant's conduct was particularly unreasonable given the nature and amount of Private
12 Information it obtained and stored and the foreseeable consequences of the immense damages that
13 would result to Representative Plaintiff and Class Members.

14 96. Defendant's violation of 15 U.S.C. § 45 constitutes negligence *per se*. Defendant
15 also violated the HIPAA Privacy and Security rules which, likewise, constitutes negligence *per se*.

16 97. As a direct and proximate result of Defendant's negligence and negligence *per se*,
17 Representative Plaintiff and Class Members have suffered and will continue to suffer injury,
18 including but not limited to (i) actual identity theft, (ii) the loss of the opportunity of how their
19 Private Information is used, (iii) the compromise, publication and/or theft of their Private
20 Information, (iv) out-of-pocket expenses associated with the prevention, detection and recovery
21 from identity theft, tax fraud and/or unauthorized use of their Private Information, (v) lost
22 opportunity costs associated with effort expended and the loss of productivity addressing and
23 attempting to mitigate the actual and future consequences of the Data Breach, including but not
24 limited to efforts spent researching how to prevent, detect, contest and recover from
25 embarrassment and identity theft, (vi) lost continuity in relation to their personal records, (vii) the
26 continued risk to their Private Information, which may remain in Defendant's possession and is
27 subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and
28 adequate measures to protect Representative Plaintiff's and Class Members' Private Information

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 in its continued possession, and (viii) future costs in terms of time, effort and money that will be
2 expended to prevent, detect, contest and repair the impact of the Private Information compromised
3 as a result of the Data Breach for the remainder of the lives of Representative Plaintiff and Class
4 Members.

5 98. As a direct and proximate result of Defendant's negligence and negligence *per se*,
6 Representative Plaintiff and Class Members have suffered and will continue to suffer other forms
7 of injury and/or harm, including but not limited to anxiety, emotional distress, loss of privacy and
8 other economic and noneconomic losses.

9 99. Additionally, as a direct and proximate result of Defendant's negligence and
10 negligence *per se*, Representative Plaintiff and Class Members have suffered and will continue to
11 suffer the continued risks of exposure of their Private Information, which remains in Defendant's
12 possession and is subject to further unauthorized disclosures so long as Defendant fails to
13 undertake appropriate and adequate measures to protect Private Information in its continued
14 possession.

15 **SECOND CLAIM FOR RELIEF**
16 **Breach of Implied Contract**
17 **(On behalf of the Nationwide Class)**

18 100. Each and every allegation of the preceding paragraphs is incorporated in this Count
19 with the same force and effect as though fully set forth herein.

20 101. Through their course of conduct, Defendant, Representative Plaintiff and Class
21 Members entered into implied contracts for Defendant to implement data security adequate to
22 safeguard and protect the privacy of Representative Plaintiff's and Class Members' Private
23 Information.

24 102. Defendant required Representative Plaintiff and Class Members to provide and
25 entrust their Private Information as a condition of obtaining Defendant's services from Defendant.

26 103. Defendant solicited and invited Representative Plaintiff and Class Members to
27 provide their Private Information as part of Defendant's regular business practices. Representative
28

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 Plaintiff and Class Members accepted Defendant’s offers and provided their Private Information
2 to Defendant.

3 104. As a condition of being direct customers and/or employees of Defendant,
4 Representative Plaintiff and Class Members provided and entrusted their Private Information to
5 Defendant. In so doing, Representative Plaintiff and Class Members entered into implied contracts
6 with Defendant by which Defendant agreed to safeguard and protect such non-public information,
7 to keep such information secure and confidential and to timely and accurately notify
8 Representative Plaintiff and Class Members if its data had been breached and compromised or
9 stolen.

10 105. A meeting of the minds occurred when Representative Plaintiff and Class Members
11 agreed to, and did, provide their Private Information to Defendant, in exchange for, amongst other
12 things, the protection of their Private Information.

13 106. Representative Plaintiff and Class Members fully performed their obligations under
14 the implied contracts with Defendant.

15 107. Defendant breached the implied contracts it made with Representative Plaintiff and
16 Class Members by failing to safeguard and protect their Private Information and by failing to
17 provide timely and accurate notice to them that their Private Information was compromised as a
18 result of the Data Breach.

19 108. As a direct and proximate result of Defendant’s above-described breach of implied
20 contract, Representative Plaintiff and Class Members have suffered and will continue to suffer (i)
21 ongoing, imminent and impending threat of identity theft crimes, fraud and abuse, resulting in
22 monetary loss and economic harm, (ii) actual identity theft crimes, fraud and abuse, resulting in
23 monetary loss and economic harm, (iii) loss of the confidentiality of the stolen confidential data,
24 (iv) the illegal sale of the compromised data on the dark web, (v) lost work time, and (vi) other
25 economic and noneconomic harm.

26
27
28

1 measures to protect Representative Plaintiff's and Class Members' Private
 2 Information from unauthorized disclosure, release, data breaches and theft,
 3 which was a direct and proximate cause of the Data Breach. Defendant
 4 failed to identify foreseeable security risks, remediate identified security
 5 risks and adequately maintain and/or improve security following previous
 6 cybersecurity incidents. This conduct, with little if any utility, is unfair
 7 when weighed against the harm to Representative Plaintiff and Class
 8 Members, whose Private Information has been compromised.

- 9 b. Defendant's failure to implement and maintain reasonable security
 10 measures, which was contrary to legislatively declared public policy that
 11 seeks to protect consumers' data and ensure that entities that are trusted with
 12 it use appropriate security measures. These policies are reflected in laws,
 13 including the FTC Act (15 U.S.C. § 45, *et seq.*).
- 14 c. Defendant's failure to implement and maintain reasonable security
 15 measures, which also leads to substantial consumer injuries, as described
 16 above, that are not outweighed by any countervailing benefits to consumers
 17 or competition. Moreover, because consumers could not know of
 18 Defendant's inadequate security, consumers could not have reasonably
 19 avoided the harms that Defendant caused.
- 20 d. Engaging in unlawful business practices by violating Cal. Civ. Code §
 21 1798.82.

22 Defendant has engaged in "unlawful" business practices by violating multiple laws,
 23 including the FTC Act, 15 U.S.C. § 45, *et seq.*, and California common law.

24 118. Defendant's unlawful, unfair and deceptive acts and practices include:

- 25 a. Failing to implement and maintain reasonable security and privacy
 26 measures to protect Representative Plaintiff's and Class Members' Private
 27 Information, which was a direct and proximate cause of the Data Breach;
- 28 b. Failing to identify foreseeable security and privacy risks, remediate
 identified security and privacy risks and adequately maintain and/or
 improve security and privacy measures, which was a direct and proximate
 cause of the Data Breach;
- c. Failing to comply with common law and statutory duties pertaining to the
 security and privacy of Representative Plaintiff's and Class Members'
 Private Information, including duties imposed by the FTC Act, 15 U.S.C. §
 45, *et seq.*, which was a direct and proximate cause of the Data Breach;
- d. Misrepresenting that it would protect the privacy and confidentiality of
 Representative Plaintiff's and Class Members' Private Information,
 including by implementing and maintaining reasonable security measures;
- e. Misrepresenting that it would comply with common law and statutory duties
 pertaining to the security and privacy of Representative Plaintiff's and Class
 Members' Private Information, including duties imposed by the FTC Act,
 15 U.S.C. § 45, *et seq.*

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

- 1 f. Omitting, suppressing and concealing the material fact that it did not
- 2 reasonably or adequately secure Representative Plaintiff's and Class
- 3 Members' Private Information; and
- 4 g. Omitting, suppressing and concealing the material fact that it did not
- 5 comply with common law and statutory duties pertaining to the security and
- 6 privacy of Representative Plaintiff's and Class Members' Private
- 7 Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, *et*
- 8 *seq.*

9 119. Defendant's representations and omissions were material because they were likely
10 to deceive reasonable consumers about the adequacy of Defendant's data security and ability to
11 protect the confidentiality of consumers' Private Information.

12 120. As a direct and proximate result of Defendant's unfair, unlawful and fraudulent acts
13 and practices, Representative Plaintiff and Class Members were injured and lost money or
14 property, including the price received by Defendant for its goods and services, monetary damages
15 from fraud and identity theft, time and expenses related to monitoring their financial accounts for
16 fraudulent activity, an increased, imminent risk of fraud and identity theft and loss of value of their
17 Private Information.

18 121. Defendant acted intentionally, knowingly and maliciously to violate California's
19 Unfair Competition Law and recklessly disregarded Representative Plaintiff's and Class
20 Members' rights.

21 122. Representative Plaintiff and Class Members seek all monetary and nonmonetary
22 relief allowed by law, including restitution of all profits stemming from Defendant's unfair,
23 unlawful and fraudulent business practices or use of their Private Information, declaratory relief,
24 reasonable attorneys' fees and costs, injunctive relief and other appropriate equitable relief.

25 **RELIEF SOUGHT**

26 **WHEREFORE**, Representative Plaintiff, on Representative Plaintiff's own behalf and on
27 behalf of each member of the proposed National Class, respectfully requests that the Court enter
28 judgment in favor of Representative Plaintiff and the Class and for the following specific relief
against Defendant as follows:

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1 1. That the Court declare, adjudge and decree that this action is a proper class action
2 and certify each of the proposed Classes and/or any other appropriate Subclasses under Federal
3 Rules of Civil Procedure Rule 23 (b)(1), (b)(2), and/or (b)(3), including appointment of
4 Representative Plaintiff's counsel as Class Counsel;

5 2. For an award of damages, including actual, nominal and consequential damages, as
6 allowed by law in an amount to be determined;

7 3. That the Court enjoin Defendant, ordering it to cease and desist from unlawful
8 activities;

9 4. For equitable relief enjoining Defendant from engaging in the wrongful conduct
10 complained of herein pertaining to the misuse and/or disclosure of Representative Plaintiff's and
11 Class Members' Private Information, and from refusing to issue prompt, complete and accurate
12 disclosures to Representative Plaintiff and Class Members;

13 5. For injunctive relief requested by Representative Plaintiff, including but not limited
14 to injunctive and other equitable relief as is necessary to protect the interests of Representative
15 Plaintiff and Class Members, including but not limited to an Order:

- 16 a. prohibiting Defendant from engaging in the wrongful and unlawful acts
17 described herein;
- 18 b. requiring Defendant to protect, including through encryption, all data
19 collected through the course of business in accordance with all applicable
20 regulations, industry standards and federal, state or local laws;
- 21 c. requiring Defendant to delete and purge Representative Plaintiff's and Class
22 Members' Private Information unless Defendant can provide to the Court
23 reasonable justification for the retention and use of such information when
24 weighed against the privacy interests of Representative Plaintiff and Class
25 Members;
- 26 d. requiring Defendant to implement and maintain a comprehensive
27 Information Security Program designed to protect the confidentiality and
28 integrity of Representative Plaintiff's and Class Members' Private
 Information;
- e. requiring Defendant to engage independent third-party security auditors and
 internal personnel to run automated security monitoring, simulated attacks,
 penetration tests and audits on Defendant's systems on a periodic basis;
- f. prohibiting Defendant from maintaining Representative Plaintiff's and
 Class Members' Private Information on a cloud-based database;

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- g. requiring Defendant to segment data by creating firewalls and access controls so that if one area of Defendant’s network is compromised, hackers cannot gain access to other portions of Defendant’s systems;
- h. requiring Defendant to conduct regular database scanning and securing checks;
- i. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees’ respective responsibilities with handling Private Information, as well as protecting the Private Information of Representative Plaintiff and Class Members;
- j. requiring Defendant to implement a system of tests to assess its respective employees’ knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees’ compliance with Defendant’s policies, programs and systems for protecting personal identifying information;
- k. requiring Defendant to implement, maintain, review and revise as necessary a threat management program to appropriately monitor Defendant’s networks for internal and external threats, and assess whether monitoring tools are properly configured, tested and updated; and
- l. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves.

- 6. For prejudgment interest on all amounts awarded, at the prevailing legal rate;
 - 7. For an award of attorneys’ fees, costs and litigation expenses, as allowed by law;
- and
- 8. For all other Orders, findings and determinations identified and sought in this

Complaint.

JURY DEMAND

Representative Plaintiff, individually and on behalf of the Plaintiff Classes and/or Subclasses, hereby demands a trial by jury for all issues triable by jury.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Dated: May 7, 2024

By: /s/ Elizabeth Ruth Klos
Scott Edward Cole, Esq. (CA S.B. #160744)
Laura Van Note, Esq. (CA S.B. #310160)
Elizabeth Klos, Esq. (CA S.B. #346781)
COLE & VAN NOTE
555 12th Street, Suite 2100
Oakland, California 94607
Telephone: (510) 891-9800
Facsimile: (510) 891-7030
Email: sec@colevannote.com
Email: lvn@colevannote.com
Email: erk@colevannote.com

*Attorneys for Representative Plaintiff and the
Plaintiff Class*

COLE & VAN NOTE
ATTORNEYS AT LAW
555 12TH STREET, SUITE 2100
OAKLAND, CA 94607
TEL: (510) 891-9800

JS-CAND 44 (Rev. 10/2020)

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

SHYRAH STRICKLAND, individually, and on behalf of all others similarly situated,

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

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

Cole & Van Note, 555 12th Street, Suite 2100, Oakland, CA 94607
Telephone: (510) 891-9800

DEFENDANTS

DROPBOX, INC.,

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

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

Attorneys (If Known)

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

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

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

	PTF	DEF		PTF	DEF
Citizen of This State	<input type="checkbox"/> 1	<input type="checkbox"/> 1	Incorporated or Principal Place of Business In This State	<input type="checkbox"/> 4	<input checked="" type="checkbox"/> 4
Citizen of Another State	<input checked="" type="checkbox"/> 2	<input type="checkbox"/> 2	Incorporated and Principal Place of Business In Another State	<input type="checkbox"/> 5	<input type="checkbox"/> 5
Citizen or Subject of a Foreign Country	<input type="checkbox"/> 3	<input type="checkbox"/> 3	Foreign Nation	<input type="checkbox"/> 6	<input type="checkbox"/> 6

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

CONTRACT	TORTS	FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
110 Insurance	PERSONAL INJURY	625 Drug Related Seizure of Property 21 USC § 881	422 Appeal 28 USC § 158	375 False Claims Act
120 Marine	310 Airplane	690 Other	423 Withdrawal 28 USC § 157	376 Qui Tam (31 USC § 3729(a))
130 Miller Act	315 Airplane Product Liability	LABOR	PROPERTY RIGHTS	400 State Reapportionment
140 Negotiable Instrument	320 Assault, Libel & Slander	710 Fair Labor Standards Act	820 Copyrights	410 Antitrust
150 Recovery of Overpayment Of Veteran's Benefits	330 Federal Employers' Liability	720 Labor/Management Relations	830 Patent	430 Banks and Banking
151 Medicare Act	340 Marine	740 Railway Labor Act	835 Patent—Abbreviated New Drug Application	450 Commerce
152 Recovery of Defaulted Student Loans (Excludes Veterans)	345 Marine Product Liability	751 Family and Medical Leave Act	840 Trademark	460 Deportation
153 Recovery of Overpayment of Veteran's Benefits	350 Motor Vehicle	790 Other Labor Litigation	880 Defend Trade Secrets Act of 2016	470 Racketeer Influenced & Corrupt Organizations
160 Stockholders' Suits	355 Motor Vehicle Product Liability	791 Employee Retirement Income Security Act	SOCIAL SECURITY	480 Consumer Credit
190 Other Contract	<input checked="" type="checkbox"/> 360 Other Personal Injury	IMMIGRATION	861 HIA (1395ff)	485 Telephone Consumer Protection Act
195 Contract Product Liability	362 Personal Injury -Medical Malpractice	462 Naturalization Application	862 Black Lung (923)	490 Cable/Sat TV
196 Franchise	CIVIL RIGHTS	465 Other Immigration Actions	863 DIWC/DIWW (405(g))	850 Securities/Commodities/Exchange
REAL PROPERTY	440 Other Civil Rights	PRISONER PETITIONS	864 SSID Title XVI	890 Other Statutory Actions
210 Land Condemnation	441 Voting	HABEAS CORPUS	865 RSI (405(g))	891 Agricultural Acts
220 Foreclosure	442 Employment	463 Alien Detainee	FEDERAL TAX SUITS	893 Environmental Matters
230 Rent Lease & Ejectment	443 Housing/Accommodations	510 Motions to Vacate Sentence	870 Taxes (U.S. Plaintiff or Defendant)	895 Freedom of Information Act
240 Torts to Land	445 Amer. w/Disabilities—Employment	530 General	871 IRS—Third Party 26 USC § 7609	896 Arbitration
245 Tort Product Liability	446 Amer. w/Disabilities—Other	535 Death Penalty		899 Administrative Procedure Act/Review or Appeal of Agency Decision
290 All Other Real Property	448 Education	OTHER		950 Constitutionality of State Statutes
		540 Mandamus & Other		
		550 Civil Rights		
		555 Prison Condition		
		560 Civil Detainee—Conditions of Confinement		

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. Code § 1332 (d)

Brief description of cause:

Defendant failed to properly secure and safeguard Plaintiff's personally identifiable information stored on Defendant's network.

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$

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 05/07/2024

SIGNATURE OF ATTORNEY OF RECORD

/s/ Elizabeth Ruth Klos

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.