MOGINRUBIN LLP
Daniel J. Mogin (SBN No. 95624)
Jennifer M. Oliver (SBN 311196)
Timothy Z. LaComb (SBN 314244)
600 West Broadway, Suite 3300
San Diego, CA 92101
Telephone: (619) 687-6611
Facsimile: (619) 687-6610
dmogin@moginrubin.com
joliver@moginrubin.com
tlacomb@moginrubin.com

SCHACK LAW GROUP
Alex Schack (SBN 99126)
16870 West Bernardo Drive, Suite 400
San Diego, CA 92127
Telephone: (858) 485-6535
Facsimile: (858) 485-0608
alexschack@schacklawgroup.com

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

MELISSA ATKINSON AND KATIE RENVALL, INDIVIDUALLY AND ON BEHALF OF CLASSES OF SIMILARLY SITUATED INDIVIDUALS,

Plaintiffs,

v.

MINTED, INC.,

Defendant.

Case No.:

COMPLAINT FOR:

(1) Violation of the California Consumer Privacy Act § 1798.150
(2) Violation of California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200, *et seq.*
(3) Negligence
(4) Breach of Contract
(5) Breach of Implied Contract

DEMAND FOR JURY TRIAL

Plaintiffs Melissa Atkinson and Katie Renvall, individually and on behalf of classes of similarly situated individuals (defined below), bring this action against Defendant Minted, Inc. ("Minted" or "Defendant"). Plaintiffs and their counsel believe that reasonable discovery will provide additional evidentiary support for the allegations herein.

I. SUMMARY OF THE CASE

1. On May 6, 2020, a computer hacking group using the pseudonym Shiny Hunters[1] burst onto the "dark web" scene when it attempted to sell more than 73.2 million records containing personally identifiable information from the user databases of eleven different companies; including Minted.

2. Minted is an online marketplace for "crowd sourced" home goods, art, and stationery, allowing independent artists to submit art that is voted on by the Minted community. The winning submissions are then sold as home décor and stationery to consumers via Minted's online platform.

3. Despite its reliance on independent artists for its artistic content, Minted is not a small business by any means. According to a 2019 feature in Inc. Magazine, Minted employs between 400 to 800 people at any given time and generates hundreds of millions of dollars in annual sales. In 2018, the company announced its series E financing, totaling $300 million of capital raised to date.

4. To purchase goods and services on Defendant's website, customers create and populate user profiles with personally identifiable information ("PII") such as first and last name, email address, password, home address, telephone number, and payment card information. Minted customers trust that their PII will be maintained in a secure manner and kept from unauthorized disclosure to third parties as outlined in Minted's Privacy Policy.[2]

1 The name "Shiny Hunter" refers to "shiny hunting," a term used by players of Pokémon games. "Shiny Hunting" is the practice of actively seeking out, capturing, and collecting rare shiny Pokémon. Here, the Shiny Hunters hunted and found eleven rare companies whose data security was weak enough to allow hackers to steal and attempt to sell millions of customer records.

2 https://www.minted.com/lp/privacy-policy; last accessed on June 10, 2020.

5. According to its notice to affected customers,[3] on May 15, 2020 Minted "became aware of a report that mentioned Minted as one of ten companies impacted by a potential cybersecurity incident" (the "Data Breach"). Minted was the subject of a hack that resulted in the attempted sale of 5 million of its customer records on the dark web, and it did not even know until learning about it in a public report.

6. Nearly two weeks later, and more than three weeks after the Data Breach occurred, Minted notified affected customers that their PII had been disclosed to unauthorized and malicious third parties.

7. To date, Minted has acknowledged that the customer information disclosed in the Data Breach included a combination of the following PII:

- name;
- email address;
- "hashed" or "salted" password; and
- where available, telephone number, billing address, and shipping address(es).

8. Minted says it has "no reason to believe that … payment or credit card information, address book information, photos or personalized information" were breached. Minted has neither confirmed that those pieces of PII were not also disclosed nor advised its customers of the basis for its stated belief that those pieces of PII were not disclosed. It is now

3 Minted's notice to affected customers was sent via email on May 28, 2020, including a phone number for customer inquiries, as required by Cal. Civ. Code section 1798.82(a). Section 1798.82(a) requires businesses to notify "any California resident (1) whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person, or, (2) whose encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person and the encryption key or security credential was, or is reasonably believed to have been, acquired by an unauthorized person and the person or business that owns or licenses the encrypted information has a reasonable belief that the encryption key or security credential could render that personal information readable or usable. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system." According to the staff reached via the phone number Minted provided in its notice, the notice was sent because Minted was "legally required" to do so.

more than one month since the Data Breach occurred, and Minted's stated position is, in effect, that it is still unsure just how much of its customers' PII was hacked.

9. The Minted customer PII disclosed in the Data Breach is protected by the California Consumer Privacy Act of 2018 ("CCPA"), which went into effect on January 1, 2020. For purposes of CCPA Section 1798.150, "personal information" is defined as an individual's first name or first initial and his or her last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (1) social security number; (2) driver's license number or California ID card number; (3) account number or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account; (4) medical information; and/or (5) health insurance information.[4]

10. When nonencrypted and nonredacted personal information defined in Section 1798.150 is subjected to unauthorized access and exfiltration, theft, or disclosure by a company that has failed to maintain reasonable security measures, the CCPA explicitly authorizes private litigants to bring individual or class action claims.[5]

11. According to Minted's notice to affected customers, the PII subjected to unauthorized access and exfiltration, theft or disclosure in the Data Breach includes (among other things): (i) customers' unencrypted and unredacted name, and (ii) an email address that serves as an account login/account number, and (iii)a hashed or salted password. In combination, those pieces of PII could permit access to other accounts using similar passwords, including financial accounts.

12. Minted has failed to maintain reasonable security controls and systems appropriate for the nature of the PII it maintains as required by the CCPA and other common

4 In other sections of the CCPA, "personal information" is defined more broadly as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

5 CCPA Section 1798.192 also states: "Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable."

and statutory laws. Hashed and "salted" passwords are not necessarily encrypted. According to one blogger for the International Association for Privacy Professionals, "encryption is a security strategy …[that] protects your organization from scenarios like a devastating breach where, if the adversary were to gain access to your servers, the data stored would be of no use to them, unless they have the encryption key. It's an all-or-nothing security posture: You either get the see the data unencrypted, or you don't."[6] "[O]rganizations should encrypt their data on a disk as a required security measure. But they must not stop there. In fact, the CCPA is clear that they should go further." *Id*.

13. Because passwords that are merely "hashed" and "salted" are not encrypted, they "can be accessed and used even while […] redacted with different levels of utility based on how much manipulating of the data is done to protect privacy." *Id.* Therefore, at a minimum, the PII disclosed in the Data Breach included user passwords that would permit sophisticated hackers like the Shiny Hunters to access to an online account.

14. Minted also failed to maintain proper measures to detect hacking and intrusion. According to its notice to affected customers, Minted did not learn that 5 million of its customer records were stolen until the hack was publicly reported. As explained below, Minted should have had breach detection protocols in place. If it had, it could have learned of the breach and alerted customers much sooner.

15. Because (i) Minted has failed to maintain reasonable security measures, and (ii) the names that Minted disclosed in combination with emails and passwords were unredacted and unencrypted, the CCPA explicitly permits an individual or class action under Section 1798.150 for this Data Breach.

16. Minted claims it is "continuing to investigate this incident diligently," is "reviewing [its] security protocols," and has "taken steps to enhance security." But the viewing, theft, and attempted sale of California consumers' PII on the dark web has already occurred and cannot be cured.

6 Tuow, Steve, *Encryption, redaction and the CCPA*, available at https://iapp.org/news/a/encryption-redaction-and-the-ccpa/ (last accessed June 10, 2020).

17. Defendant disregarded Plaintiffs' and Class members' privacy rights in the PII by, among other things, (i) failing to implement reasonable security safeguards to prevent or timely detect the Data Breach; (ii) failing to disclose to customers that it did not implement such reasonable security safeguards; and (iii) failing to provide sufficiently prompt, thorough, and accurate notice and information concerning the Data Breach.

18. As a result of the Data Breach, Plaintiffs and the Classes have been injured in several ways. Plaintiffs and Class members (i) now know or should know that their PII was hacked and put up for sale on the dark web for purchase by malicious actors; (ii) face an imminent and ongoing risk of identity theft and similar cyber crimes; (iii) have expended and will continue to expend time and money to protect against cyber crimes; (iv) have lost value in their PII; and (v) did not receive the benefit of their bargain with Defendant regarding data privacy.

19. Plaintiffs and Class members are therefore (i) entitled to actual and statutory damages under the CCPA and other laws, (ii) have incurred actual and concrete damages as a result of the unauthorized sale of their PII to malicious actors on the dark web, and (iii) face ongoing risks of disclosure of their PII in subsequent data breaches because Defendant has not demonstrated that it has implemented reasonable security systems and procedures. Plaintiffs and Class members have a significant interest in the protection and safe storage of their PII. They are therefore entitled to declaratory, injunctive, and other equitable relief necessary to protect their PII. This includes, but is not limited to, an order compelling Defendant to adopt reasonable security procedures and practices to safeguard customers' PII and prevent future data breaches.

II. JURISDICTION AND VENUE

20. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and one or more members of the Classes are residents of a different state than Defendant Minted. The Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

21. This Court has personal jurisdiction over Defendant because it has continuous and systematic contacts with and conducts substantial business in the State of California and this

District. Defendant maintains its principal place of business in this District and has continuous and systematic contacts with and conducts substantial business in the State of California and this District.

22. Venue is proper in this District pursuant to 28 U.S.C. §1391(b). A substantial part of the events giving rise to these claims took place in this District, numerous Class members reside in this District and were therefore harmed in this District.

Intradistrict Assignment

23. There is no basis for assignment to a particular location or division of the Court pursuant to Civil L.R. 3-2(c). This civil action arose in the county of San Francisco and a substantial part of the events or omissions that give rise to the claims herein occurred in San Francisco.

III. PARTIES

24. Plaintiffs Melissa Atkinson and Katie Renvall are natural persons and permanent, non-transitory residents of the State of California. Like millions of others, Ms. Atkinson and Ms. Renvall created user profiles on Minted's website and entrusted Minted with their PII. On May 28, 2020, Ms. Atkinson and Ms. Renvall received an email from Minted notifying them that their PII had been accessed by malicious third parties without authorization. Because of the Data Breach, they have continuously monitored their various accounts to detect misuse of their PII and will continue to expend time to protect against fraudulent use or sale of their PII.

25. Defendant Minted is a for-profit Delaware corporation and maintains a headquarters and principal place of business at 747 Front Street, Suite 200, San Francisco, CA 94111. Minted operates an online design marketplace with millions of customers and hundreds of millions of dollars in gross annual revenue.

IV. FACTUAL BACKGROUND

Defendant's Relevant Privacy Policies

26. Minted's Privacy Policy is available on its website and provides customers with terms and conditions regarding the treatment of their PII. For example, it states:

- You may choose to give us your contact information during registration or at other times. We then may use that information to contact you about the products and services on our site. **Registration is required to use certain interactive features such as reviewing products, saving designs, and placing orders.**
- Registration allows a user to utilize 'saved design' functionality on the Website. Users may customize a virtually unlimited number of stationery items. The text on these **saved designs may contain personal information including addresses, contact information, dates of personal events or any other personal information you provide. This information is only available to the registered user and Minted staff.**
- We collect information you provide to us. For example, we collect personal identifiers such as your name and email address from you when you register for a Minted account, so that you can create a log in to access your account. When you place an order**, we collect your phone number, email address, billing and shipping address and credit card information**, so that we can fulfill your order and ship your product or product samples. **We may also collect information you provide as part of selecting your preferences, including within your account settings, and commercial information, such as the Minted products you have purchased or offered for sale.**
- If you participate in Minted as an artist, in addition to the above we may **collect your signature and education for purposes of offering and promoting your products on the Minted platform** and applying your signature to manufactured products, and your **financial information for purposes of paying commissions or reimbursements.**
- We also collect any information you voluntarily provide to us, which may include your **date of birth and protected characteristics such as your age and gender** to customize products, as well as visual information such as **photographs and images you upload** (and, if you participate in Minted as an artist, any video and audio recordings you provide). If you participate in our user testing, we collect **recordings of you user testing session** (with your consent) [sic].
- We may also collect and store information about other people that you provide to us when you use our services, including without limitation **email and mailing addresses of family and friends** (for example, when you submit a guest list for an event for the purpose of creating customized invitations), and any such information you store is personal information.
- We may also automatically collect certain information about how you access or use the Website and our services including,

> but not limited to, information about your **internet domain address, clickstream information, IP address, browsing history, and other electronic markers and identifiers**. We also collect imprecise geolocation information as implied by your IP address. We collect **inferences drawn from your shopping preferences and other activity on our Website**. We may also collect information through the use of cookies, web beacons and similar technologies and use third-party service providers that may use cookies, web beacons and similar technologies to help operate their services.
>
> - We also collect information from partners such as service providers (including data licensors, analytics providers, and payment processors), public databases, our marketing partners, and advertisers. This may include **information about your interests, demographic data, purchasing behavior, and your activities online** (such as websites visited and advertisements viewed). We use this to better understand your preferences and interests, and to **customize content and advertisements** for you.

27. Minted's Privacy Policy reveals the significant benefit Minted derives from collecting and maintaining its customers PII. In addition to the uses listed above, Minted uses its customers' PII for:

- "Improving [its] Services, including testing, research, internal analytics, and product development;"
- "Understanding how users interact with the Website and [its] Services;"
- "Personalizing website content and communications based on your preferences;"
- "Providing a better website experience and gathering broad demographic information for aggregate use;"
- "Marketing and selling [its] Services;" and
- "Showing [its consumers] advertisements, including interest-based or online behavioral advertising."

28. Minted's Privacy Policy assures Minted customers their PII is secure. For example, Minted states it will "not rent, sell, or share [customers'] personal information with other people or non-affiliated companies except to provide products or services that [the

customer has] requested, or unless we have [the customer's] permission as agreed in this Policy or otherwise, or as set forth in the California Privacy Rights section below."

29. The "California Privacy Rights section" is a statement for purposes of compliance with the CCPA, including that if "there are any conflicts between this section and any other provision of this Privacy Policy and you are a California resident, the portion that is more protective of personal information shall control to the extent of such conflict."

30. Despite these assurances and the significant benefit Minted receives by collecting and maintaining its customers' PII, Minted did not adopt reasonable data measures and systems to protect customers' PII or prevent and detect unauthorized access to this data. Minted maintains a business that operates exclusively online and collects hundreds of millions of dollars from online customers each year; it has the resources to adopt reasonable protections and should have known to do so. It knew or should have known that its systems had inadequate protections that placed its customers at significant risk of having their PII stolen by hackers.

31. Minted requires its customers to provide PII when using its website to purchase goods or services. It collects, retains, and uses that data to maximize profits through predictive marketing and other targeted marketing practices. By collecting, using, and deriving significant benefit from customers' PII, Minted had a legal duty to take reasonable steps to protect this information from disclosure. As discussed below, Defendant also had a legal duty to take reasonable steps to protect customers' PII under applicable federal and state statutes, including Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, and the California Consumer Protection Act of 2018 (the "CCPA"), Cal. Civ. Code § 1798, *et seq.*

FTC Security Guidelines Concerning PII

32. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches.

33. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures to protect PII by companies like Defendant. Several publications by the FTC outline the

importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

34. In 2016, the FTC provided updated security guidelines in a publication titled *Protecting Personal Information: A Guide for Business*. Under these guidelines, companies should protect consumer information they keep; limit the sensitive consumer information they keep; encrypt sensitive information sent to third parties or stored on computer networks; identify and understand network vulnerabilities; regularly run up-to-date anti-malware programs; and pay particular attention to the security of web applications – the software used to give information to visitors to a company's website and to retrieve information from the visitors.

35. The FTC recommends that businesses refrain from maintaining payment card information beyond the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

36. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

37. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website:

> When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In

> addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.

38. Minted was aware or should have been aware of its obligations to protect its customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers from unauthorized access. Among other violations, Minted violated its obligations under Section 5 of the FTC Act.

39. For example, Minted's uncertainty regarding whether its customers' payment card information was disclosed in this Data Breach indicates that it is maintaining payment card information on its systems beyond the time necessary to process payments.

40. Likewise, Minted's admission that it did not learn of the breach until it was publicly reported more than a week later indicates that it does not use an adequate intrusion detection system to immediately expose a data breach; does not sufficiently monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; does not properly monitor for the transmission of large amounts of data from the system; and does not maintain an appropriate plan to respond effectively to a data breach in the event one occurs.

The Data Breach Harmed Plaintiffs and Class Members

41. Plaintiffs and Class members have suffered and will continue to suffer harm because of the Data Breach.

42. Plaintiffs and Class members face an imminent risk of injury of identity theft and related cyber crimes due to the Data Breach. Once data is stolen, malicious actors will either exploit the data for profit themselves or sell the data on the dark web, as occurred here, to someone who intends to exploit the data for profit. Hackers would not incur the time and effort to steal PII and then risk prosecution by listing it for sale on the dark web if the PII was not valuable to malicious actors.

43. The dark web helps ensure users' privacy by effectively hiding server or IP details from the public. Users need special software to access the dark web. Most websites on the dark web are not directly accessible via traditional searches on common search engines and are therefore accessible only by users who know the addresses for those websites.

44. Malicious actors use PII to gain access to Class members' digital life, including bank accounts, social media, and credit card details. During that process, hackers can harvest other sensitive data from the victim's accounts, including personal information of family, friends, and colleagues.

45. Malicious actors can also use Class members' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."

46. The PII accessed in the Data Breach therefore has significant value to the hackers that have already sold or attempted to sell that information and may do so again. In fact, names, mailing and email addresses, dates of birth, phone numbers, account information, and purchasing preferences are among the most valuable pieces of information for hackers.

47. The PII accessed in the Data Breach is also very valuable to Minted. Minted collects, retains, and uses this information to increase profits through predictive and other targeted marketing campaigns. Minted customers value the privacy of this information and expect Minted to allocate enough resources to ensure it is adequately protected. Customers would not have done business with Minted, uploaded personal address books and photos, provided payment card information, and/or paid the same prices for Minted's goods and services had they known Minted did not implement reasonable security measures to protect their PII. Minted's holiday cards and wedding invitations can cost customers $5 or more per card. Customers expect that those premium prices incorporate Minted's operating costs, including costs to implement reasonable security measures to protect customers' personal information.

48. The PII accessed in the Data Breach is also very valuable to Plaintiffs and Class members. Consumers often exchange personal information for goods and services. For example, consumers often exchange their personal information for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (*e.g.*, sign-up coupons exchanged for email addresses). Consumers use their unique and valuable PII to access the financial sector, including when obtaining a mortgage,

credit card, or business loan. As a result of the Data Breach, Plaintiffs and Class members' PII has been compromised and lost significant value.

49. Plaintiffs and Class members will face a risk of injury due to the Data Breach for years to come. Malicious actors often wait months or years to use the personal information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. For example, victims often do not know that certain accounts have been opened in their name until contacted by collections agencies. Plaintiffs and Class members will therefore need to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them.

50. Plaintiffs and Class members have and will continue to expend significant time and money to reduce the risk of and protect against identity theft caused by the Data Breach. According to the 2018 IBM/Ponemon Institute study, the average cost of a data breach in the United States is $242 per victim and roughly $8 million per breach for companies. Where a consumer becomes a victim of identity theft and suffers $1 or more in direct or indirect losses, the average cost to the consumer is $1,343.

51. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud. On average, victims of identity theft spend 7 hours fixing issues caused by the identity theft. In some instances, victims spend more than 1,000 hours trying to fix these issues.

52. Victims of identity theft also experience harm beyond economic effects. According to a 2018 study by the Identity Theft Resource Center, 32% of identity theft victims experienced negative effects at work (either with their boss or coworkers) and 8% experienced negative effects at school (either with school officials or other students).

53. The U.S. Government Accountability Office likewise determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."

Defendant Failed to Take Reasonable Steps to Protect its Customers' PII

54. As stated above, Minted requires its customers to provide a significant amount of highly personal and confidential PII to purchase its good and services. Defendant collects, stores, and uses this data to maximize profits.

55. Minted has legal duties to protect its customers' PII by implementing reasonable security features. This duty is further defined by federal and state guidelines and industry norms.

56. Defendant breached its duties by failing to implement reasonable safeguards to ensure Plaintiffs' and Class members' PII was adequately protected. As a direct and proximate result of this breach of duty, the Data Breach occurred, and Plaintiffs and Class members were harmed. Plaintiffs and Class members did not consent to having their PII disclosed to any third-party, much less a malicious hacker who would sell it on the dark web.

57. The Data Breach was a reasonably foreseeable consequence of Defendant's inadequate security systems. Defendant Minted, which made approximately $150 million in revenue in 2019, has the resources to implement reasonable security systems to prevent or limit damage from data breaches. Even so, it failed to properly invest in its data security. If Minted had implemented reasonable data security systems and procedures (*i.e.*, followed guidelines from industry experts and state and federal governments), then it likely could have prevented hackers from infiltrating its systems and accessing its customers' PII.

58. Minted's failure to implement reasonable security systems has caused Plaintiffs and Class members to suffer and continue to suffer harm that adversely impact Plaintiffs and Class members economically, emotionally, and/or socially. As discussed above, Plaintiffs and Class members now face an imminent and ongoing threat of identity theft and resulting harm. These individuals now must spend significant time and money to continuously monitor their

accounts and credit scores to limit potential adverse effects of the Data Breach regardless of whether any Class member ultimately falls victim to identity theft.

59. Defendant also had a duty to timely discover the Data Breach and notify Plaintiffs and Class members that their PII had been compromised. Defendant breached this duty by failing to use reasonable intrusion detection measures to identify the Data Breach when it occurred, and then, once it learned of the Data Breach nine days later, failing to inform affected customers for an additional thirteen days. For twenty-two days between the Data Breach and Minted's notification to customers, customers' PII was in the hands of hackers and for sale to malicious actors.

60. In sum, Plaintiffs and Class members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) diminution in value of their PII; (iv) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (v) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; and (vi) overpayments to Minted for goods and services purchased, as Plaintiffs and Class members reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII, which was not the case.

61. Minted has failed to recognize the impact of the Data Breach on its customers; it has not even offered impacted customers credit monitoring services or other mitigation measures beyond what is available to the public. For example, Minted's notice to affected customers states that they "may obtain a free copy of [their] credit report from each of the three credit reporting agencies … [or] … request information regarding fraud alerts, security freezes, and identity theft from the following credit reporting agencies," but "fees may be involved for some of these services."

62. Even if Minted had offered monitoring or other services to its affected customers, it would be insufficient to protect Plaintiffs and Class members. As discussed above, the threat of identity theft and fraud from the Data Breach will extend for years and cost Plaintiffs and the Classes significant time and effort. Minted's notice to affected customers acknowledges this,

encouraging customers to "change [their] password at your earliest convenience," "change [their] password for any other online accounts for which [they] use the same email address and password combination," "be cautious of any unsolicited communications that ask [them] to provide [their] personal information electronically and avoid clicking on links or downloading attachments from suspicious emails."

63. Plaintiffs and Class members therefore have a significant and cognizable interest in obtaining equitable relief (in addition to any monetary damages) that protects them from these long-term threats.

V. CLASS ACTION ALLEGATIONS

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

1. The Nationwide Class: All individuals whose PII was compromised in the Data Breach; and

2. The California Class: All persons residing in California whose PII was compromised in the Data Breach.

65. Specifically excluded from the Classes are Defendant; its officers, directors or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir or assign of Defendant. Also excluded from the Classes are attorneys and staff of law firms participating in this matter and the members of his or her immediate family, any federal, state or local governmental entities, any judicial officer presiding over this action and the members of his or her immediate family and judicial staff, and any juror assigned to this action.

66. The members of the Classes are so numerous that joinder of all members is impracticable. While the exact number of class members in each of the Classes is unknown to Plaintiffs at this time and can only be ascertained through appropriate discovery, it has been reported that the Data Breach affected approximately 5 million customers nationwide. California makes up roughly 12% of the nation's population and is believed to be home to a

disproportionate number of Minted customers relative to other states. It is therefore believed that the California Class consists of 750,000 or more Class members and the Nationwide Class consists of 5 million or more Class members.

67. Plaintiffs' claims are typical of the claims of the members of the Classes. All Class members were subject to the Data Breach and had their PII exposed or accessed in the Data Breach. Likewise, Defendant's misconduct impacted all Class members in the same manner.

68. Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs' interests are aligned with Class members' interests because they were subject to the same Data Breach as Class members and face similar threats as a result of the Data Breach. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions.

69. Defendant has acted in a manner that applies generally to Plaintiffs and all Class members. Each Class member has been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect customers' PII, as well as Defendant's failure to timely alert affected customers of the Data Breach.

70. Common questions of law and fact predominate over questions affecting individual Class members. The common questions of fact and law include:

(a) whether Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and Class members' PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information;

(b) whether Defendant's misconduct identified herein amounts to a violation of Cal. Bus. & Prof. Code § 17200, *et seq.*;

(c) whether Defendant owed Plaintiffs and Class members a duty to implement and maintain reasonable security procedures and practices to protect their personal information;

(d) whether Defendant breached its duty to implement reasonable security systems to protect Plaintiffs' and the Class members' PII;

(e) whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and Class members;

(f) whether Defendant provided timely notice of the Data Breach to Plaintiffs and Class members;

(g) whether, prior to the Data Breach, Defendant knew or should have known that its security systems were vulnerable to the type of cyber-attack that led to the Data Breach; and

(h) whether Class members are entitled to compensatory damages, punitive damages, statutory or civil penalties, and/or injunctive relief as a result of the Data Breach.

71. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all Class members is impracticable. The individual prosecution of separate actions by individuals would lead to repetitive adjudication of common questions and fact and law and create a risk of inconsistent or varying adjudications that would establish incompatible standards of conduct for Defendant. There will be no difficulty in the management of this action as a class action.

VI. CLAIMS ALLEGED ON BEHALF OF THE CALIFORNIA CLASS

COUNT I
Violation of the CCPA, Cal. Civ. Code § 1798.150

72. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

73. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and Class members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

74. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect this personal information. As identified herein, Defendant failed to do so. As a direct and proximate result of Defendant's acts, Plaintiffs' and Class members' personal information, including unencrypted names, emails and passwords among other information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

75. Plaintiffs and Class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant

continues to hold customers' PII, including Plaintiffs' and Class members' PII. These individuals have an interest in ensuring that their PII is reasonably protected.

76. On June 9, 2020, Plaintiffs' counsel sent a notice letter to Minted's registered service agent via UPS Next Day Air. Plaintiffs' counsel also emailed a copy of the notice to the help@minted.com email address on June 11. Assuming Minted cannot cure the Data Breach within 30 days, and Plaintiffs believe such cure is not possible under these facts and circumstances, then Plaintiffs intend to promptly amend this complaint to seek actual damages and statutory damages of $750 per customer record subject to the Data Breach on behalf of the California Class as permitted by the CCPA.

COUNT II
Violation of California's Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.*

77. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

78. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, *et seq*.

79. As alleged herein, Defendant engaged in the following unlawful and/or unfair conduct: (i) violation of the CCPA; (ii) negligence; (iii) negligence *per se*; (iii) breach of contract; and (v) breach of implied contract.

80. As also alleged herein, Plaintiffs and Class members were directly and proximately harmed in several ways as a result of Defendant's unlawful and/or unfair conduct. Defendant is liable to Plaintiffs and Class members for those damages.

VII. CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

COUNT III
Negligence

81. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

82. Defendant owed Plaintiffs and Class members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access. Defendant breached its duty of care by failing to implement reasonable security procedures and practices to protect Plaintiffs' and Class members' PII. Defendant failed to, *inter alia*: (i) implement security systems and practices consistent with federal and state guidelines; (ii) implement security systems and practices consistent with industry norms; (iii) timely detect the Data Breach; and (iv) timely disclose the Data Breach to impacted customers.

83. Minted knew or should have known Plaintiffs' and Class members' PII was highly sought after by hackers and that Plaintiffs and Class members would suffer significant harm if their PII was stolen by hackers.

84. Defendant also knew or should have known that timely disclosure of the Data Breach was required and necessary to allow Plaintiffs and Class members to take appropriate actions to mitigate the resulting harm. These efforts include, but are not limited to, freezing accounts, changing passwords, monitoring credit scores/profiles for fraudulent charges, contacting financial institutions, and cancelling or monitoring government-issued IDs such as passports and driver's licenses. The risk of significant harm to Plaintiffs and Class members (including identity theft) increased as the amount of time between the Data Breach and disclosure lengthened to reach a full twenty-two days.

85. Defendant had a special relationship with Plaintiffs and the Class members who entrusted Defendant with several pieces of PII. Customers were required to provide PII when utilizing Defendant's properties and/or services. Plaintiffs and Class members were led to believe Defendant would take reasonable precautions to protect their PII and would timely inform them if their PII was compromised, but the Defendant did not do so.

86. The harm that Plaintiffs and Class members suffered (and continue to suffer) was the reasonably foreseeable product of Defendant's breach of its duty of care. Defendant failed to enact reasonable security procedures and practices and Plaintiffs and Class members were the foreseeable victims of data theft that exploited the inadequate security measures. The PII

accessed in the Data Breach is precisely the type of information that hackers seek and use to commit cyber crimes.

87. But for Defendant's breach of its duty of care, the Data Breach would not have occurred and, therefore, Plaintiffs' and Class members' PII would not have been accessed and put up for sale by an unauthorized and malicious party.

Negligence *Per Se*

88. As alleged above, Defendant owed a duty to Plaintiffs and Class members to exercise reasonable care in safeguarding their PII from being compromised, lost, stolen, accessed or misused by unauthorized persons. Defendant also owed Plaintiffs and Class members a duty to timely disclose any unauthorized access and theft of PII so that they could take appropriate measures to mitigate the adverse consequences caused by the Data Breach.

89. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45) and related FTC publications, Defendant has a duty to Plaintiffs and Class members to provide fair and adequate data security practices to safeguard Plaintiffs' and Class members' PII. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, failing to use reasonable measures to protect PII.

90. Pursuant to Section 1798.150 of the CCPA, Defendant has a duty to Plaintiffs and Class members to implement and maintain reasonable security procedures and practices to protect their PII.

91. Defendant violated the FTC Act and the CCPA by failing to use reasonable security measures to protect PII and not complying with applicable industry, federal and state guidelines and standards. Defendant's conduct was particularly unreasonable given the nature and amount of customer PII it stored and the foreseeability and resulting consequences of a data breach.

92. Plaintiffs and Class members are part of the Class of persons the FTC Act and CCPA were intended to protect. The harm that was proximately caused by the Data Breach is the type of harm the FTC Act and CCPA were intended to guard against. The FTC has brought

enforcement actions against entities that, due to a failure to employ reasonable data security measures, caused the same harm as that suffered by Plaintiffs and Class members here.

93. Defendant's negligence *per se* directly and proximately caused Plaintiffs and the Class to suffer (and continue to suffer) damages. These damages include, but are not limited to, identity theft and the corresponding costs, significantly heightened risk of identity theft for the next several years, and time and effort spent mitigating the effects of the Data Breach.

COUNT V

Breach of Contract

94. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

95. Defendant knew of or should have known that Plaintiffs' and Class members' PII they provided was highly confidential and sensitive.

96. Defendant's Privacy Policy is an agreement between Defendant and customers who provide PII to Defendant, which includes Plaintiffs and Class members.

97. According to Defendant's Privacy Policy, individuals are subject to its terms when they "us[e] the Website or any of the Services [Defendant] provide[s]."

98. Customers (including Plaintiffs and Class members) give certain PII to Defendant when they use Defendant's website and purchase items or services from Defendant. Plaintiffs and Class members therefore demonstrated their willingness and intent to enter into a bargain with Defendant and assent to the terms of the Privacy Policy by giving their PII to Defendant.

99. Defendant demonstrated its intent to adhere to its obligations under the Privacy Policy and related statements when collecting Plaintiffs' and Class members' PII, including promising to "not rent, sell, or share [customers'] personal information with other people or non-affiliated companies except to provide products or services that [the customer has] requested, or unless we have [the customer's] permission."

100. Plaintiffs and Class members therefore entered into a contract with Defendant when providing PII to Defendant subject to the terms of the Privacy Policy.

101. Plaintiffs and Class members upheld their obligations under the agreement. Defendant, on the other hand, breached its obligations by failing implement reasonable security measures to ensure that it would not inadvertently "share [customers'] personal information with other people or non-affiliated companies," which led to unauthorized disclosure of PII to third parties.

102. As a direct and proximate result of Defendant's breach of this agreement, Plaintiffs and Class members did not receive the benefit of their bargain with Defendant and were injured, as described in detail herein.

COUNT VI
Breach of Implied Contract

103. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

104. Plaintiffs and Class members entered into an implied contract with Defendant by providing PII to Defendant when utilizing services provided by and/or purchasing goods from Defendant. Implied in these exchanges, Defendant agreed to implement reasonable procedures and practices to protect the PII of Plaintiffs and Class Members and to timely notify them in the event the PII was compromised.

105. Plaintiffs and Class members reasonably expected that Defendant had implemented adequate security measures to protect their PII and would allocate a portion of the money paid by Plaintiffs and Class members under the implied contracts to fund those security measures.

106. Neither Plaintiffs nor Class members would have provided their PII to Defendant or paid the same fees to Defendant for goods and services without the implied contract between them and Defendant. Defendant needed to adequately safeguard Plaintiffs' and Class members' PII and provide timely notice of a data breach to realize the intent of the parties.

107. Plaintiffs and Class members performed their obligations under the implied agreements with Defendant. Conversely, Defendant breached its obligations under the implied contracts by (i) failing to implement reasonable security procedures and practices to protect

Plaintiffs' and Class members' PII; (ii) enabling unauthorized access of PII by third parties due to the inadequate security measures; and (iii) failing to provide timely notice of the Data Breach.

108. As a direct and proximate result of Defendant's breaches of its implied contract, Plaintiffs and Class members did not get the benefit of their implied contract with Defendant and were injured as described in detail above.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Classes, requests the following relief:

A. A determination that this action is a proper class action under Federal Rule of Procedure Rule 23, certifying Plaintiffs as Class representatives, and appointing the undersigned counsel as Class counsel;

B. An award of compensatory damages, punitive damages, statutory or civil penalties to Plaintiff and the Classes as warranted by applicable law;

C. Injunctive or other equitable relief that directs Defendant to implement reasonable security procedures and practices to protect customers' PII that conform to relevant federal and state guidelines and industry norms;

D. Awarding Plaintiffs and the Classes reasonable costs and expenses incurred in this action, including attorneys' fees and expert fees; and

E. Such other relief as the Court may deem just and proper.

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

/ / /

IX. JURY DEMAND

Plaintiffs demand a trial by jury on all issues so triable as a matter of right.

DATED: June 11, 2020

/s/ *Jennifer M. Oliver*

MOGINRUBIN LLP
Daniel J. Mogin
Jennifer M. Oliver
Timothy Z. LaComb
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: (619) 687-6611
Facsimile: (619) 687-6610

SCHACK LAW GROUP
Alex Schack
16870 West Bernardo Drive, Suite 400
San Diego, CA 92127
Telephone: (858) 485-6535
Facsimile: (858) 485-0608

Attorneys for Plaintiffs

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
Melissa Atkinson, Katie Renvall,
individually and on behalf of classes of similarly situated individuals,

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

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
MoginRubin LLP, Jennifer M. Oliver (SBN311196), 600 W. Broadway, San Diego, CA 92101, 619-687-6611

DEFENDANTS
Minted, 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)*
(For Diversity Cases Only)

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

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

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

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

TORTS

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

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

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

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

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

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

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

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

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

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

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent–Abbreviated New Drug Application
- ☐ 840 Trademark

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

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

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

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

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

VI. CAUSE OF ACTION
Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332
Brief description of cause:
Unlawful business practices concerning personal data use and distribution.

VII. REQUESTED IN COMPLAINT:
✓ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.
DEMAND $ 5,000,000.00
CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

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

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)
(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 06/11/2020 **SIGNATURE OF ATTORNEY OF RECORD** /s/Jennifer M. Oliver