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

SCHACK LAW GROUP
Alexander M. Schack, Esq., Bar No. 99126
Natasha N. Serino, Esq., Bar No. 284711
Shannon F. Nocon, Esq., Bar No. 316523
16870 West Bernardo Drive, Suite 400
San Diego, CA 92127
Tel: (858) 485-6535
Fax: (858) 485-0608
alexschack@schacklawgroup.com
natashaserino@schacklawgroup.com
shannonnocon@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.: 3:20-cv-03869-VC

FIRST AMENDED 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) Declaratory and Injunctive Relief

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"). This Amended Complaint is filed pursuant to Fed. R. Civ. P. 15(a).

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 over 73.2 million records containing personally identifiable information from the user databases of eleven 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.

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 initial 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 over three weeks after public reports of the Data Breach and sale of customer records on the dark web, Minted finally 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: names, login credentials, email address, hashed and salted passwords (some of which were decoded into full text passwords), telephone number, billing address, shipping address(es), the last four digits of credit card numbers, and for some affected customers, date of birth.

8. Although the passwords disclosed were hashed and salted, Minted has confirmed ***"that unauthorized actors may have later determined plain text passwords for some accounts."*** Minted has not confirmed that address book information, photos, or personalized information were not also disclosed.

3 Minted's first notice to affected customers was sent via email on May 28, 2020. It included 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.

9. The Minted customer PII disclosed in the Data Breach is protected by the California Consumer Privacy Act of 2018 ("CCPA"). 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. Here, unencrypted names were revealed along with account information and passwords that would permit access to individuals' financial and other accounts across the web. 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, in combination with (ii) an email address (iii) other login credentials that serve as an account login/account number, and (iv) a hashed or salted password that allowed hackers to obtain full text passwords. In combination, those pieces of PII could permit access to other accounts using similar or the same usernames, emails, and/or passwords, including financial accounts. Many consumers use the same emails and passwords across numerous online accounts, including financial accounts.

11. 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

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."

litigants to bring individual or class action claims.[5] Minted consumers whose passwords were cracked suffered especially great harm; hackers almost certainly got into many of their accounts across the internet. When a consumers' password is revealed, hackers gain a key to their entire online life: retirement accounts, bank accounts, social media profiles, email, and more. Users who employ common passwords are typically the least sophisticated and also the most vulnerable: they are the most likely to use the same password across accounts, and the most likely to use less complex passwords that are easier to crack. Successful theft of passwords—especially when it goes unnoticed or unreported for some time as was the case here—is among the most devastating hacks that a consumer can suffer.

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 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 to 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.* For example, it is possible to

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."

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).

"replay" a hashed password without ever determining the original plain text password. Depending on the systems in use, simply obtaining a hashed password can be enough information to permit hackers to access a user's account. Therefore, at a minimum, the PII disclosed in the Data Breach included user passwords that would, and did, permit sophisticated hackers like the Shiny Hunters access to customers' other online accounts using similar credentials.

14. Minted's latest update to its data breach notice acknowledges this is exactly what occurred in the Data Breach; the hackers obtained full passwords for many customers. Minted's failure to implement a reasonable security policy of requiring strong passwords only exacerbated the risk to its customers. At the time of the Data Breach, Minted users were permitted to employ a weak six-digit password with no capital letters or special characters, making it even easier for hackers to decode them.

15. 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.

16. Nearly all "best practices" security frameworks, *e.g.*, the U.S. National Institute of Standards and Technology's (NIST) Special Publication 800, require log aggregation, log monitoring, and automated intrusion detection systems that alert a company of unauthorized access or the anomalous use of hacked user accounts. Had Minted properly deployed those industry standard systems, the breach might not have occurred or, if it had, Minted would have promptly detected it.

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

18. 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.

19. 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 detect the Data Breach when or after it occurred; (iii) failing to disclose to customers that it did not implement such reasonable security safeguards; and (iv) failing to provide sufficiently prompt, thorough, and accurate notice and information about the Data Breach.

20. 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.

21. 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

22. This Court has jurisdiction over this action under 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 under 28 U.S.C. § 1367.

23. 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.

24. Venue is proper in this District under 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

25. 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

26. 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.

27. 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. The acts alleged to have been done by Defendant were authorized, ordered, or performed by its directors, officers, managers, agents, employees, or representatives in the course of their employment and while actively engaged in the management of Defendant's affairs. Defendant, through its subsidiaries, divisions, affiliates and agents, operated as a single unified entity with each acting as the agent or joint-venturer of or for the others regarding the acts, violations, and common course of conduct alleged herein and under the authority and apparent authority of parent entities, principals and controlling parties.

IV. CLASS ACTION ALLEGATIONS

28. Plaintiffs bring this nationwide class action under 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.

29. 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.

30. 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.

31. 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.

32. 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.

33. 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 to the Data Breach.

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

(e) whether Defendant adequately addressed and fixed vulnerabilities that permitted the Data Beach to occur;

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

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

(h) whether and when Defendant learned of the Data Breach and whether the response was adequate;

(i) whether Plaintiffs and other Class members are entitled to credit monitoring and other injunctive relief;

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

(k) 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

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

35. 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 of 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.

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

37. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues the resolution of which would

advance this matter and the parties' interests therein. These issues include, but are not limited to:

(a) whether Defendant owed a legal duty to Plaintiffs and Class members to exercise due care in collecting, storing, using and safeguarding their PII;

(b) whether Defendant failed to comply with its own policies and applicable laws, regulations and industry standards relating to data security;

(c) whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach; and

(d) whether Plaintiffs and Class members are entitled to actual damages, credit monitoring, other injunctive relief, and/or punitive damages because of Defendant's wrongful conduct.

V. FACTUAL BACKGROUND

Defendant's Relevant Privacy Policies

38. 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.

39. 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."

40. 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." By failing to protect its customers' PII through reasonable security measures, Minted has shared personal information with others for purposes other than the services customers requested without customers' permission.

41. 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."

42. 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. The protections afforded by implementing the best practices delineated in modern security practices frameworks are not unduly expensive for a company like Minted and are commonly deployed by commercial businesses throughout the world. It knew or should have known that its systems' inadequate protections placed its customers at significant risk of having their PII stolen by hackers.

43. 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

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

45. 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.

46. 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 inform visitors to a company's website and to retrieve information from the visitors.

47. The FTC recommends that businesses do not maintain 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.

48. 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.

49. 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.

50. 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.

51. For example, Minted's initial 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.

52. 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

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

54. 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.

55. 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.

56. 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.

57. 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."

58. 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.

59. 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.

60. 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.

61. 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 rarely 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.

62. 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.

63. 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.

64. 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).

65. 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

66. 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.

67. 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.

68. 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.

69. 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. Had Minted 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.

70. 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.

71. 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.

72. 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.

73. 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."

74. 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."

75. 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. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

VI. CLAIMS ALLEGED ON BEHALF OF THE CALIFORNIA CLASS

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

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

77. Plaintiffs and the California Class members hereby seek relief under § 1798.150(a), including, but not limited to, (i) recovery of actual damages or damages in an amount not less than $100 and not greater than $750 per consumer per incident, whichever is greater, (ii) injunctive or declaratory relief, and (iii) any other relief the Court deems proper, including attorneys' fees and costs pursuant to Cal. Code Civ. P. § 1021.5.

78. Plaintiffs and Class members also 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.

79. Defendant is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues over $25 million. Defendant collected consumers' PII as defined in Cal. Civ. Code § 1798.140.

80. 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.

81. 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.

82. Plaintiffs have made several failed and successful attempts to serve Defendant Minted with notice and opportunity to cure pursuant to Cal. Civ. Code §1798.150: (i) on June 9, 2020, Plaintiffs' counsel sent the notice letter to Minted's registered service agent via UPS Next Day Air, which UPS could not deliver after several attempts; (ii) on June 11, 2020, Plaintiffs' counsel emailed a copy of the notice letter to help@minted.com; and (iii) on June 17, 2020, Plaintiffs' counsel served a copy of the notice letter via email to counsel authorized to accept service of Plaintiffs' complaint.

83. Defendant has not responded to Plaintiffs' Cal. Civ. Code §1798.150 letter. Specifically, Defendant failed to (i) provide an express written statement that the violations have been cured and that no further violations shall occur as required by § 1798.150; or (ii) "actually cure" its violation of Cal. Civ. Code §1798.150(a) within thirty days of Plaintiffs' written notice of Defendants' violation of §1798.150(a).

84. Over thirty days have elapsed since Plaintiffs served a notice and opportunity to cure letter pursuant to Cal. Civ. Code §1798.150 on Defendant Minted. Over thirty days have also elapsed since Plaintiffs served their first complaint. Plaintiffs' claim for statutory damages under the CCPA is therefore proper.

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

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

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

87. Defendant engaged in unlawful acts and practices by maintaining sub-standard security practices and procedures as described herein, by soliciting collecting and profiting from Plaintiffs' and Class members' PII knowing that it would not be adequately protected, and by storing Plaintiffs' and Class members' PII in an unsecure electronic environment in violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires Defendant to implement and maintain reasonable security procedures and practices to safeguard the PII of Plaintiffs and the Class.

88. In addition, Defendant engaged in unlawful acts and practices by failing to disclose the Data Breach to the Plaintiffs and the Class in a timely and accurate manner contrary to the duties imposed by Cal. Civ. Code §1798.82. When Defendant finally did make the legally required disclosure, it did not include the "Notice of Data Breach" language required by the §1798.82. Instead, the communication was titled "Notice of Data Security Incident."

89. As alleged herein, Defendant engaged in negligence, among other unfair acts and practices. Plaintiffs and Class members were directly and proximately harmed in several ways as a result of Defendant's unlawful and/or unfair conduct and are entitled to all available injunctive relief, including but not limited to an order mandating Defendant (i) implement reasonable security measures to protect its customers' PII and (ii) provide free credit monitoring to customers affected by the Data Breach.

VII. CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

COUNT III
Negligence

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

91. 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.

92. Defendant 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.

93. 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.

94. 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. Defendant had a duty to protect that information. 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, and the Defendant breached its duty when it failed to do so.

95. 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.

96. 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*

97. 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.

98. 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.

99. 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.

100. 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.

101. 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.

102. 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.

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 and civil penalties to Plaintiff and the Classes as warranted by the CCPA and other applicable law;

C. Injunctive or other equitable relief that directs Defendant to provide Plaintiffs and the Classes with free credit monitoring and to implement reasonable security procedures and practices to protect customers' PII that conform to relevant federal and state guidelines and industry norms;

D. Declaratory judgement in favor of Plaintiffs determining that Defendant's failure to implement reasonable security measures violates the CCPA;

E. An award of reasonable costs and expenses incurred in prosecuting this action, including attorneys' fees and expert fees pursuant to Cal. Code Civ. P. § 1021.5; 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: July 27, 2020

/s/Jennifer M. Oliver

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

SCHACK LAW GROUP
Alexander M. Schack, Esq., Bar No. 99126
Natasha N. Serino, Esq., Bar No. 284711
Shannon F. Nocon, Esq., Bar No. 316523
16870 West Bernardo Drive, Suite 400
San Diego, CA 92127
Tel: (858) 485-6535
Fax: (858) 485-0608
alexschack@schacklawgroup.com
natashaserino@schacklawgroup.com
shannonnocon@schacklawgroup.com

Attorneys for Plaintiffs