MATTHEW RIGHETTI (SBN: 121012)
matt@righettilaw.com
JOHN GLUGOSKI (SBN: 191551)
jglugoski@righettilaw.com
MICHAEL RIGHETTI (SBN: 258541)
RIGHETTI GLUGOSKI, P.C.
456 Montgomery Street. Suite 1400
San Francisco, CA 94104
Tel: (415) 983-0900
Fax: (415) 397-9005

Gretchen Nelson (SBN: 112566)
gnelson@nflawfirm.com
Gabriel S. Barenfeld (SBN: 224146)
gbarenfeld@nflawfirm.com
NELSON & FRAENKEL LLP
601 So. Figueroa Street, Suite 2050
Los Angeles, CA 90017
Phone: (844) 622-6469
Fax: (213) 622-6019

Attorneys for Plaintiffs and the Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA
IN AND FOR THE COUNTY OF SAN FRANCISCO

RICHARD DANIELE, RICHARD GOSS and STEVE LANDI, individually, and on behalf of a class of similarly situated persons,

Plaintiffs,

v.

10UP, INC., a California Corporation; and DOES 1-50 inclusive,

Defendants.

Case No. CGC-20-586506

CLASS ACTION

FIRST AMENDED COMPLAINT FOR:

(1) VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT (Civil Code, § 1798.150, *et seq*)

(2) NEGLIGENCE

(3) VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW (Bus. & Prof. Code, § 17200)

DEMAND FOR JURY TRIAL

Plaintiffs Richard Daniele, Richard Goss and Steve Landi bring this lawsuit against 10UP, Inc., and DOES 1 through 50 (together "Defendant" or "10UP"), on behalf of themselves and all others similarly situated ("Class" or "Class Members"), for violation of their privacy rights. Plaintiffs allege, upon personal knowledge as to their own actions, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. San Francisco Employees' Retirement System (SFERS) oversees and administers a retirement plan for approximately 74,000 active and retired employees of the City and County of San Francisco. Since 2016, SFERS has contracted with 10UP to provide SFERS members[1] with, among other things, online access to their account information. In such capacity, 10UP receives and obtains personal identifiable information ("PII")[2] of SFERS members.

2. On or about February 24, 2020, 10UP was the target of a massive data breach in which approximately 74,000 SFRERS members were subject to an unauthorized access and exfiltration, theft, or disclosure of their PII ("Data Breach"). Outside parties accessed a trove of personal details about SFERS members—such as names, home addresses, dates of birth, designated beneficiary information, 1099-R tax form information, bank account routing numbers, and SFERS website usernames and passwords—stored on one of 10UP's servers. 10UP maintained the highly sensitive PII in a form that was neither encrypted nor redacted.

3. In addition to violating the fundamental privacy rights of Plaintiffs and Class Members, the Data Breach has caused them to suffer ongoing economic damages and other actual damages. Because of the Data Breach, they face an increased risk of identity theft and concomitant expenses associated with mitigating that risk. Plaintiffs and Class Members require

---

[1] As used herein, the term "SFERS members" includes both current and former SFERS members and is intended to be limited to those members who fall within the "Class" definition, as set forth below.

[2] As used herein, the term "PII" is intended to include the definition of personal information provided under Civil Code sections 1798.140, subdivision (o), and 1798.81.5, subdivision(d)(1).

robust credit monitoring services and software to reasonably mitigate the danger of future identity theft and fraud.

4. Plaintiffs bring this lawsuit on behalf of Class Members whose PII was compromised as a result of the Data Breach and 10UP's failure to (i) implement and maintain reasonable security procedures and practices appropriate to the nature of the PII; (ii) disclose its inadequate security procedures and practices; (iii) effectively monitor its systems for security vulnerabilities; and (iv) timely detect, report, and disclose the Data Breach.

5. 10UP's conduct, as alleged herein, was negligent, constitutes an unfair business practice under California's Unfair Competition Law (Bus. & Prof. Code, § 17200) ("UCL"), and violates the California Consumer Privacy Act of 2018 (Civil Code, § 1798.150, *et seq*) ("CCPA"), among other violations.

II. PARTIES

6. At all relevant times, Plaintiff Richard Daniele was and is a citizen of California, residing in San Francisco County. Plaintiff Daniele is a retiree and member of SFERS. He entrusted his PII to SFERS, which, in turn, entrusted it to 10UP. Plaintiff Daniele's nonencrypted or nonredacted PII was subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the Data Breach. This resulted in an invasion of his privacy interests, loss of value of his PII, and has placed him at imminent, immediate, and continuing risk of further identity theft-related harm. Plaintiff Daniele has spent money on a credit monitoring service as part of a reasonable effort to mitigate against such harm and will continue to incur such expenses on an ongoing basis.

7. At all relevant times, Plaintiff Richard Goss was and is a citizen of California, residing in San Francisco County. Plaintiff Goss is a retiree and member of the SFERS. Plaintiff Goss entrusted his PII to SFERS who, in turn, entrusted it to 10UP. Plaintiff Goss's nonencrypted or nonredacted PII was subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the Data Breach. This resulted in an invasion of his privacy interests, loss of value of his PII, and has placed him at imminent, immediate, and continuing risk of further identity theft-related harm.

8. At all relevant times, Plaintiff Steve Landi was and is a citizen of California, residing in San Francisco County. Plaintiff Landi is a retiree and member of SFERS. He entrusted his PII to SFERS, which, in turn, entrusted it to 10UP. Plaintiff Landi's nonencrypted or nonredacted PII was subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the Data Breach. This resulted in an invasion of his privacy interests, loss of value of his PII, and has placed him at imminent, immediate, and continuing risk of further identity theft-related harm. For example, in approximately July of 2020, Richard Daniele's wife was notified about suspicious debit/credit card activity.

9. Defendant 10UP, Inc. is a private corporation that was founded in 2011 and incorporated in California, in 2014. 10UP maintains its headquarters and does business in California and is organized or operated for the profit or financial benefit of its shareholders or other owners. According to its website, 10UP specializes in "digital strategy and management, software engineering, user experience and interactive design, cloud infrastructure, and audience and revenue optimization." (https://10up.com [as of August 24, 2020].) 10UP claims to "make the web better by finely crafting websites & tools for content creators." (*Ibid.*)

10. Plaintiffs do not know the true names and capacities of Defendants sued herein as Does 1 through 50, inclusive, and therefore sues these defendants by such fictitious names. Plaintiffs are informed and believe that each of the Doe defendants was in some manner legally responsible for the damages alleged below. Plaintiffs will amend this Complaint to set forth the true names and capacities of these defendants when ascertained, along with appropriate charging allegations.

11. Plaintiffs are informed and believe, and thereupon allege, that each of the defendants designated herein as a Doe is responsible in some actionable manner for the events and happenings referred to herein, and caused injuries to Plaintiffs, as hereinafter alleged, either through said defendants' conduct, or through the conduct of their agents, servants, employees. The term "Defendant(s)" as used in this Complaint includes both the named Defendant and Defendants sued under the fictitious names of Does 1 through 50, inclusive.

12. Plaintiffs are informed and believe and therefore alleges that, at all times

relevant to this action, Defendants, and each of them, were the agents, servants, employees, assistants, and consultants of each of their co-Defendants, and were, as such, acting within the course of and scope of the authority of their agency and employment, and that each and every Defendant when acting as a principal, was negligent and careless in the selection and hiring of each and every co-Defendant as an agent, servant, employee, assistant and/or consultant.

III. JURISDICTION AND VENUE

13. This Court has personal jurisdiction over 10UP because it is headquartered in California and conducts a major part of its operations with regular and continuous business activity in California. The claims of Plaintiffs and the Class arise out of 10UP's business activity in California and, at all times herein mentioned, 10UP was performing services pursuant to a contract entered into and performed in California.

14. Venue is proper in this Court because a substantial part of the events or omissions giving rise to these claims occurred in, were directed to, and/or emanated from San Francisco. Venue is also proper because 10UP entered into a contract with the City and County of San Francisco, pursuant to which it was entrusted with the PII of SFERS Members. Venue is also proper under Business & Professions Code section 17203.

15. This is a class action brought pursuant to Code of Civil Procedure section 382, and this Court has jurisdiction over the Plaintiffs' claims because the amount in controversy exceeds this Court's jurisdictional minimum.

16. Federal jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d) is lacking. Two-thirds or more of the members of the proposed Class, in the aggregate, and the primary defendant is a citizen of the State of California. (28 U.S.C. § 1332(d)(4)(B).) Alternatively, federal jurisdiction under the Class Action Fairness Act is lacking because greater than two-thirds of all the proposed plaintiff class members are citizens of California; at least one of the defendants from whom significant relief is sought and whose alleged conduct forms a significant basis for the claims, is a citizen of California; and the principal injuries resulting from the alleged conduct or any related conduct of each defendant were incurred in California.

IV. FACTUAL ALLEGATIONS

17. SFERS entered into one or more contracts with 10UP (together, "Contracts"), starting on or about October 4, 2016, for "strategic consulting services," wherein 10UP agreed to "[d]evelop and implement functional modules to add to the existing SFERS website and member portal, etc." 10 UP, under its Contracts, collects or receives the PII of SFERS members and alone, or jointly with others, determines the purposes and means of the processing of such PII. 10UP, under its Contracts, took possession, retained, stored, and maintained a database containing the PII of Plaintiffs and Class Members.

18. As stated in the Notice of Data Breach sent by SFERS, 10UP set up "a test environment on a separate computer server which included a database containing data from approximately 74,000 SFERS member accounts as of August 29, 2018."[3] On information and belief, at all relevant times, 10UP has had annual gross revenues in excess of twenty-five million dollars ($25,000,000), and/or alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices.

19. On or about February 24, 2020, 10UP was the target of a widespread Data Breach in which nonredacted and nonencrypted PII of SFERS members that was stored on that server was subject to an unauthorized access and exfiltration, theft, or disclosure. According to SFERS, "an outside party" accessed the server, and SFERS warned that it could not confirm the PII was not copied.

20. In the Notice of Data Breach, SFERS reported that it was not told of the Data Breach until March 21, 2020, nearly a month after it occurred.

21. As set forth in the Notice of Data Breach, the compromised PII of Plaintiffs and the Class Members includes, without limitation, the following categories of highly sensitive information: (1) Full Name; (2) Full Home Address; (3) Date of Birth; (4) Designated

---

[3] See SFERS Data Breach Notice, <https://mysfers.org/wp-content/uploads/2020/06/10up-Breach-SFERS-Notice-Website-FINAL.pdf> (accessed July 17, 2020.)

Beneficiary Full Name (if any); (5) Designated Beneficiary Date of Birth; (6) Designated Beneficiary Relationship to Member; (7) IRS Form 1099R Information, excluding SSN; (8) Bank ABA (routing) Number; and (9) SFERS Website User Name, Security Questions and Answers. Plaintiffs have an increased risk of identity theft based on the nature of their PII that had been maintained on 10UP's compromised server.

22. The Data Breach subjected Plaintiffs and the other Class Members nonencrypted or nonredacted PII to an unauthorized access and exfiltration, theft, or disclosure, including, but not limited to, PII that falls within the definition of subparagraph (A) of paragraph (1) of subdivision (d) of Civil Code section 1798.81.5. Following the Data Breach, SFERS warned members, including Plaintiffs, that their "personal financial information may be misused."

23. The Data Breach resulted from 10UP's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the PII.

On information and belief, 10UP breached its standard of care by failing to implement reasonable security procedures to adequately protect Class Members' PII—which was not password protected, redacted, or encrypted—from data breaches. Data breaches, such as this one, are commonly made possible through a vulnerability in a system or server.

24. As a result of 10Up's lax security, outside parties have accessed Plaintiffs' and Class Members' PII in a readily usable form that is potentially of great value to them. Plaintiffs and Class Members are thus exposed to criminals seeking to use the PII for nefarious and illegal activities, such as identity theft schemes. Given the sensitive nature of the PII, Plaintiffs and Class Members face an immediate, concrete, and ongoing risk of identity theft and fraud.

25. At all relevant times, 10UP knew, or reasonably should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including the significant costs, damages and harm that would be imposed on Plaintiffs and the Class.

26. Over the past several years, large data breaches, such as the one that occurred

here, have garnered widespread media attention and have been the focus of protective legislation and scrutiny by law enforcement and the media. Ignoring the known risk, 10UP's approach to maintaining the security of the PII of Plaintiffs and Class Members, including, without limitation, failing to, at a minimum, encrypt or password protect such information, was well-below the standard of care.

27. State and federal agency guidelines strongly encourage encrypting information stored on computer networks and servers. In fact, failure to adequately and reasonably protect PII, as 10UP has failed to do for Plaintiffs and members of the Class, is an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

28. As a result of the Data Breach, Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiffs and the Class are also subject to a higher risk of phishing and pharming, where hackers exploit information they have already obtained in an effort to procure even more PII. Moreover, Plaintiffs and the Class now run the risk of unauthorized individuals creating credit cards in their names, taking out loans in their names, and engaging in other fraudulent conduct using their identities. Further, Plaintiffs and Class Members have experienced a loss of value of their PII as a result of the Data Breach. Given that Class Members are currently at risk of identity theft or credit fraud, prophylactic measures, such as the purchase of credit monitoring services and software, are reasonable and necessary to prevent and mitigate future loss.

California Recognizes the Importance of Protecting PII

29. The CCPA affords California residents security protections and rights to learn about and control how a business handles their personal information. The Legislature requires businesses to implement adequate standards to protect PII:

> It is the intent of the Legislature to ensure that personal information about California residents is protected. To that end, the purpose of this section is to encourage businesses that own, license, or maintain personal information about Californians to provide reasonable security for that information.

(Civ. Code, § 1798.81.5, subd. (a)(1).)

30. The CCPA further endows on California residents the right to bring an action for statutory damages if their information is subject to a data breach that is "a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information." (Civil Code, § 1798.150.)

31. The City and County of San Francisco likewise recognize the importance of protecting PII. Section 12M.2 of the San Francisco Administrative Code precludes a City contractor who, like 10UP, receives PII from the City of San Francisco in connection with a City contract from disclosing that information to "any other person or entity." And, under Section 12M.3, a violation of that provision constitutes, among other things, a material breach of the City contract.

PII Is Valuable to Hackers and Thieves

32. Hackers and criminals recognize the value of PII. Identity thieves use stolen PII for a variety of crimes, including credit card fraud, phone or utilities fraud, and financial fraud. PII can also be sold on the dark web or used to clone a credit card.

33. Once hackers obtain access to PII, it can then be used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. Other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family and friends.

34. Access to PII provides criminals further opportunity to hack into email accounts. Since most online accounts require an email address, not only as a username but also to verify accounts and reset passwords, a hacked email account can provide access to additional identity theft opportunities.

35. Hacked PII also allows thieves to obtain other personal information through "phishing." According to the Report on Phishing available on the United States, Department of Justice's website: "AT&T, a large telecommunications company, had its sales system hacked into, resulting in stolen order information including full names and home addresses, order numbers, and credit card numbers. The hackers then sent each customer a highly

personalized e-mail indicating that there had been a problem processing their order and re-directing them to a spoofed website where they were prompted to enter further information, including birthdates and Social Security numbers."[4]

36. Industry experts have reported that one in every three people who is notified of being a potential fraud victim becomes one. In the case of a data breach, simply reimbursing a consumer for a financial loss due to identity theft and fraud does not necessarily make that individual whole. The Department of Justice's Bureau of Justice Statistics ("BJS") has found, "among victims who had personal information used for fraudulent purposes" a significant percentage of victims spent a month or more resolving problems, with some even taking more than year.[5]

37. A person whose PII has been obtained and compromised may not know or experience the full extent of identity theft or fraud for years. In addition, a victim may not become aware of fraudulent charges when they are nominal because typical fraud-prevention algorithms fail to capture such charges. Those charges may be repeated, over and over, without detection.

Annual Monetary Losses from Identity Theft are in the Billions of Dollars

38. Losses from identity theft reached $21 billion in 2013. (*See* 2013 Javelin Strategies Identity Fraud Report.) According to the BJS, an estimated 17.6 million people were victims of one or more incidents of identity theft in 2014.

39. There often can be a time lag between the theft of PII and when the harm occurs or is discovered. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for

---

[4] https://www.justice.gov/archive/opa/docs/report_on_phishing.pdf (accessed on August 24, 2020).

[5] "Victims of Identity Theft," U.S. Department of Justice, Dec 2013, available at https://www.bjs.gov/content/pub/pdf/vit12.pdf (accessed on August 24, 2020).

up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[6]

Plaintiffs and Class Members Have Suffered Ongoing Damages

40. As a direct and proximate result of the Data Breach caused by 10UP's wrongful actions and inaction, Plaintiffs and Class Members have been placed at an imminent and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate any actual or potential impact of the Data Breach. Plaintiffs and Class Members now must reasonably incur the ongoing expense of surveilling their financial and personal records and monitoring. They are subject to a higher risk of phishing and pharming schemes, through which hackers exploit the ill-gotten PII to procure additional private information. In addition, Plaintiffs and Class Members run the risk of unauthorized individuals creating credit cards in their names, taking out loans in their names, and engaging in other fraudulent conduct using their identities.

41. The Data Breach has caused Plaintiffs and Class Members to suffer ongoing economic damages and other actual harm for which they are entitled to compensation, including, but not limited to, the following:

(i) lost or diminished value of PII;

(ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII;

(iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach, including, but not limited to, loss of time;

(iv) deprivation of rights under the UCL and CCPA; and

(v) an increased risk to their PII, which has been compromised and thus (a) is subject to criminal access and abuse; and (b) remains in 10UP's possession and

---

[6] See GAO, Report to Congressional Requesters, at 33 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (accessed on August 24, 2020).

is subject to further unauthorized disclosures so long as 10UP fails to undertake appropriate and adequate measures to protect the PII.

V. CLASS ALLEGATIONS

42. Plaintiffs bring this action on their own behalf and on behalf of a class of individuals pursuant to CCP 382. Plaintiffs intends to seek certification of a class defined as follows:

> **All SFERS members and former members residing in California whose PII was accessed or otherwise compromised in the Data Breach, which, according to the Notice of Data Breach provided by SFERS, occurred on or about February 24, 2020.**

Excluded from the Class are the following individuals and/or entities: Defendants and their parents, subsidiaries, affiliates, officers and directors, current or former employees, and any entity in which Defendants have a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

43. **Numerosity**. The members of the Class are so numerous that joinder of all Class Members is impractical. While the exact number of Class Members is unknown to Plaintiffs at this time, given the number of SFERS members in California and information provided by SFERS about the Data Breach, the number of Class Members is at least in the tens of thousands. Class Members are readily identifiable from information and records maintained by 10UP and SFERS.

44. **Commonality and Predominance.** This action involves questions of law and fact common to Class Members that predominate over any questions affecting individual Class Members. These common questions of law and fact include, without limitation:

a. When 10UP actually learned of the Data Breach;

b. Whether 10UP adequately detected, disclosed and responded to the Data Breach;

c. Whether 10UP owed a duty to the Class to exercise due care in collecting, encrypting, password protecting, storing, safeguarding and/or maintaining their PII;

d. Whether 10UP implemented and maintained reasonable security procedures and practices appropriate to the nature of the PII;

e. Whether 10UP breached its duty of care;

f. Whether 10UP knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class Members' PII secure and prevent loss or misuse of that PII;

g. Whether 10UP adequately addressed and fixed the vulnerabilities that permitted the Data Breach to occur;

h. Whether 10UP caused Plaintiffs and Class Members to incur damages;

i. Whether 10UP violated the law by failing to promptly notify Class Members that their PII had been compromised;

j. Whether Plaintiffs and the other Class Members are entitled to credit monitoring and other monetary relief;

k. Whether Defendants violated California's UCL;

l. Whether Class Members are entitled to statutory damages, special or general damages, civil penalties and/or injunctive relief; and

m. Whether 10UP violated CCPA by failing to maintain reasonable security procedures and practices appropriate to the nature of the PII.

45. **Typicality**: Plaintiffs' claims are typical of those of other Class Members because all had their PII accessed and compromised as a result of the Data Breach, due to 10UP's wrongful conduct, acts, or omissions.

46. **Adequacy**: Plaintiffs' interests are not antagonistic and do not irreconcilably conflict with the interests of the Class. Plaintiffs are represented by attorneys who are

competent and experienced in consumer and privacy-related class action litigation.

47. **Superiority and Manageability**: A class action is superior to other available group-wide methods for the fair and efficient adjudication of this controversy because the individual damage and harm suffered by each individual Class Member may be relatively small compared to the expense and burden of prosecuting such an individual case, and the difficulty of discovering and remedying the wrongdoing of 10UP. If individual Class Members were required to bring separate actions, courts would be confronted by a multiplicity of lawsuits burdening the court system while also creating the risk of inconsistent rulings and contradictory judgments. In contrast to proceeding on a case-by-case basis, in which inconsistent results will magnify the delay and expense to all parties and the court system, this class action presents far fewer management difficulties while providing unitary adjudication, economies of scale and comprehensive supervision by a single court.

48. 10UP has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or declaratory relief appropriate with respect to the Class as a whole.

49. Likewise, certain issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether 10UP owed a legal duty to Plaintiffs and the Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

b. Whether 10UP breached a legal duty to Plaintiffs and the Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;

c. Whether 10UP failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether 10UP has 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

e. Whether Class Members are entitled to actual damages, statutory damages,

credit monitoring or other injunctive relief, as a result of 10UP's wrongful conduct.

50. Notice of the pendency of and any resolution of this action can be provided to the Class members by individual mailed notice or the best notice practicable under the circumstances.

FIRST CAUSE OF ACTION

[Violation of the California Consumer Privacy Act ("CCPA"), Cal. Civil Code Sec. 1798.150, et seq.]

51. Plaintiffs re-allege herein all of the allegations contained in paragraphs 1 through 50, and allege against 10UP and DOES 1 through 50 (together, "Defendants") as follows.

52. Civil Code section 1798.150, subdivision (a)(1), provides,

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> > (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual damages, whichever is greater.
> >
> > (B) Injunctive or declaratory relief.
> >
> > (C) Any other relief the court deems proper.

53. On information and belief, 10UP took possession, retained, stored, and maintained a database containing the nonencrypted and nonredacted PII of Plaintiffs and the Class. 10 UP, under its Contracts, collects or receives such information and alone, or jointly with others, determines the purposes and means of the processing of such PII.

54. On or about February 24, 2020, 10UP was the target of a widespread Data Breach in which nonredacted and nonencrypted PII of Plaintiffs and approximately 74,000 Class Members that was stored on that server was subject to an unauthorized access and exfiltration, theft, or disclosure.

55. On information and belief, at all relevant times, 10UP has had annual gross revenues in excess of twenty-five million dollars ($25,000,000), and/or alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices.

56. The Data Breach subjected Plaintiffs and the other Class Members to an unauthorized access and exfiltration, theft, or disclosure of their nonencrypted and nonredacted PII, including, but not limited to, PII that falls within the definition of subparagraph (A) of paragraph (1) of subdivision (d) of Civil Code section 1798.81.5.

57. The Data Breach was a result of 10UP's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

58. Due to the Data Breach, Plaintiffs and the Class Members have suffered injury in fact and monetary damages, in an amount to be proven at trial, but in excess of the minimum jurisdictional amount of this Court.

59. Plaintiffs seek to recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per Class Member per incident or actual damages, whichever is greater; injunctive or declaratory relief; and/or any other relief the court deems proper.

60. Prior to filing this CCPA claim, Plaintiffs each provided thirty days written notice to 10UP, "identifying the specific provisions of the CCPA the consumer [Plaintiffs] allege[] have been or are being violated." 10UP could not and did not cure the violation within the time provided under the CCPA; compensate Plaintiffs or otherwise provide any remedy for the harm caused by the violation.

SECOND CAUSE OF ACTION

[Negligence]

61. Plaintiffs re-allege herein all prior allegations, and allege against Defendants as follows.

62. Defendants owed a duty to Plaintiffs and Class Members to exercise reasonable care in obtaining, using, and protecting their PII from unauthorized third parties.

63. Among other things, under both the Contracts and under Section 12M.2 of the San Francisco Administrative Code, 10UP had a duty to take reasonable measures to protect the PII of Plaintiffs' and the members of the Class.

64. The duties owed by Defendants to Plaintiffs and Class Members include, but are not limited to, the following:

a) To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting the PII of Plaintiffs and Class Members within its possession;

b) To protect PII of Plaintiffs and Class Members in its possession by using reasonable and adequate data security practices and procedures, including, but not limited to, password protecting the PII that was on its servers; and

c) To implement practices and procedures to quickly detect and timely act on data breaches, including promptly notifying SFERS and Plaintiffs and Class Members of the data breach.

65. Defendants breached their duties owed to Plaintiffs and Class Members. Defendants knew or should have known the risks of maintaining and storing PII and the importance of maintaining secure systems.

66. Defendants knew or should have known that their security procedures and practices did not adequately safeguard Plaintiffs' and the other Class Members' PII. Defendants also failed to timely detect the Data Breach and failed to encrypt, redact, and password protect the Class Members' PII.

67. Through Defendants' acts and omissions described in this Complaint,

Defendants failed to provide adequate security to protect the PII of Plaintiffs and the Class from being accessed and compromised.

68. Defendants breached the duties it owed to Plaintiffs and Class Members in several ways, including:

a) Failing to implement adequate and reasonable security systems, protocols, and practices sufficient to protect Class members' PII, which includes failing to password protect or encrypt the information on the compromised server, resulting a foreseeable risk of harm;

b) Failing to comply with the minimum industry security standards for data security;

c) Failing to act despite knowing or having reason to know that Defendants' systems were vulnerable to attacks; and

d) Failing to timely and accurately disclose to SFERS and Plaintiffs and Class Members that their PII was captured, accessed, exfiltrated, stolen, disclosed, viewed, and/or misused.

69. Due to Defendants' conduct, Plaintiffs and Class Members require, among other things, extended credit monitoring. The Data Breach creates an increased risk for identity theft and other types of financial fraud against the Class members. The consequences of identity theft are serious and long-lasting. There is a benefit to early detection and monitoring.

70. As a result of Defendants' negligence, Plaintiffs and Class Members suffered injuries and damages that include and/or may include: (i) the lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and/or recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the data breach; (iv) the continued risk to their PII, which can be subject to further unauthorized access and disclosure; (v) future costs in terms of time, effort, and money that will be expended to prevent, monitor, detect, contest, and/or repair the impact of the PII compromised as a result of the Data Breach, including ongoing credit monitoring.

71. These injuries, which also include an invasion of privacy rights, were reasonably foreseeable given the history of security breaches of this nature. The injury and harm that Plaintiffs and Class Members suffered was the direct and proximate result of Defendants' negligent conduct.

THIRD CAUSE OF ACTION

[Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code §17200]

72. Plaintiffs re-allege herein all prior allegations, and allege against Defendants as follows.

73. Defendants have engaged and continue to engage in acts and practices of unfair competition, as that term is defined in Business & Professions Code section 17200, including unlawful, unfair or fraudulent business acts or practices.

74. Defendants engaged in unlawful acts and practices by failing to implement reasonable and adequate data security practices and procedures, as described herein, by obtaining Plaintiffs' and Class members' PII with knowledge that the information would not be adequately protected; by storing Plaintiffs' and Class members' PII in an unsecure electronic environment; and by failing to timely detect and report the Data Breach.

75. Defendants have violated Civil Code section 1798.81.5, which requires Defendants to take reasonable methods of safeguarding the PII of Plaintiffs and the Class Members.

76. Defendants also engaged in unlawful acts and practices, by failing to disclose the data breach, including to Class Members in a timely and accurate manner, which violates Civil Code section 1798.82. To date, Defendants have still not provided full and accurate information regarding the Data Breach to Plaintiffs and the Class Members.

77. Defendants have further violated Section 12M.2 of the San Francisco Administrative Code, which requires Defendants to take reasonable methods of safeguarding the PII of Plaintiffs and the Class Members.

78. Defendants' business practices are unfair under the UCL because they have

acted in a manner that is unethical, oppressive, and/or substantially injurious to Plaintiffs and the Class Members. The exposure of their PII to third parties is substantially injurious because of the significant harm that can result. The harmful impact of Defendants' practice far outweighs any possible countervailing benefits.

79. On information and belief, Defendants received money or property to protect PII, for the benefit of Plaintiffs and the Class, but failed to implement adequate security policies and practices.

80. As a result of Defendants' unlawful or unfair business practices as alleged herein, Plaintiffs suffered injury in fact and lost money or property. Among other things, Plaintiffs and Class Members are entitled to recover the price received by Defendants for the services described herein, the loss of Class Members' legally protected interest in the confidentiality and privacy of their PII, and additional losses as described above.

81. Defendants knew or should have known that its computer systems and data security practices and procedure were inadequate to safeguard Class members' PII and that the risk of a data breach or theft was likely.

82. Pursuant to Business & Professions Code §§ 17203 and 17204, the Court may enjoin such conduct in the future on behalf of the Class and the general public; obtain a provision for a corrective notice; and compel Defendants to restore to Plaintiffs and Class Members any money or property that Defendants may have acquired or retained as a result of any act or practice that constitutes unfair competition. Plaintiffs further seeks an order requiring Defendants to disgorge any profits Defendants may have obtained as a result of their conduct.

83. Plaintiffs seek restitution to Plaintiffs and Class Members of money or property that Defendants may have acquired by means of their business practices alleged herein, including monetary restitution and restitutionary disgorgement of all profits accruing to Defendants because of such practices, declaratory relief, attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5), and injunctive or other equitable relief. Plaintiffs and Class Members also lost legally protected interest in the confidentiality and privacy of their PII, and

suffered additional losses as described above.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against the 10UP and that the Court grant the following:

A. An order certifying the Class as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. An order enjoining 10UP from engaging in the wrongful conduct alleged herein concerning disclosure and inadequate protection of Plaintiffs' and Class Members' PII;

C. An order instructing Defendants to purchase or provide funds for adequate credit monitoring services for Plaintiffs and all Class Members;

D. An award of compensatory and statutory damages, in an amount to be determined, including statutory damages pursuant to the CCPA;

E. An award for equitable relief and restitution as a result of 10UP's wrongful conduct;

F. An award of reasonable attorneys' fees, costs, and litigation expenses, as allowable by law;

G. Nominal damages; and

H. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial of all issues so triable.

Respectfully Submitted,

DATED: December 8, 2020

NELSON & FRAENKEL LLP

Gabriel Barenfeld

Gretchen Nelson
Gabriel Barenfeld
Attorney for Plaintiff

RIGHETTI GLUGOSKI, P.C.
Matthew Righetti
John Glugoski
Michael Righetti

Attorneys for Plaintiffs