JASON M. WUCETICH (STATE BAR NO. 222113)
jason@wukolaw.com
DIMITRIOS V. KOROVILAS (STATE BAR NO. 247230)
dimitri@wukolaw.com
WUCETICH & KOROVILAS LLP
222 N. Pacific Coast Hwy., Suite 2000
El Segundo, CA 90245
Telephone: (310) 335-2001
Facsimile: (310) 364-5201

Attorneys for Plaintiff
JUDE OKPALA, individually and on behalf of all others similarly situated

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

JUDE OKPALA, as an individual and on behalf of all others similarly situated,

Plaintiff,

v.

TRANS UNION LLC; and DOES 1-10,

Defendants.

CASE NO.

CLASS ACTION

COMPLAINT FOR:

(1) VIOLATION OF FAIR CREDIT REPORTING ACT, 15 U.S.C. § 1681 *et seq.*
(2) NEGLIGENCE
(3) NEGLIGENCE PER SE
(4) DECLARATORY JUDGMENT
(5) VIOLATION OF THE CAL. UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200
(6) VIOLATION OF THE RIGHT TO PRIVACY, CAL. CONST. ART. 1, § 1

DEMAND FOR JURY TRIAL

SUMMARY OF THE CASE

1. This putative class action arises from Trans Union LLC's (hereinafter "TU" or "Defendant") negligent failure to implement and maintain reasonable cybersecurity procedures that resulted in a data breach of its systems, which was reported on or around November 7, 2022. The breach affected nearly 200 million TransUnion customers throughout the United States. Plaintiff brings this class action to redress injuries related to the data breach, on behalf of himself and a nationwide class and California subclass of similarly situated persons. Plaintiff asserts claims for violation of the Fair Credit Reporting Act ("FCRA"), negligence, negligence per se, declaratory judgment, common law invasion of privacy, and violation of California's Unfair Competition Law ("UCL"). Plaintiff seeks, among other things, compensatory damages, statutory damages, punitive and exemplary damages, injunctive relief, attorneys' fees, and costs of suit.

PARTIES

2. Plaintiff Jude Okpala is a citizen and resident of the State of California whose personal identifying information was part of the data breach that is the subject of this action.

3. On information and belief, defendant Trans Union LLC is a consumer reporting agency organized under the laws of the State of Delaware with its principal place of business in Chicago, Illinois.

4. Plaintiff brings this action on behalf of himself, on behalf of the general public as a Private Attorney General pursuant to California Code of Civil Procedure § 1021.5 and on behalf of a class and subclass of similarly situated persons pursuant Federal Rule of Civil Procedure 23.

JURISDICTION & VENUE

5. This Court has general personal jurisdiction over TU because, at all relevant times, the company had systematic and continuous contacts with the State of California. TU is registered to do business in California with the California Secretary of State. Defendant regularly contracts with a multitude of businesses, organizations and consumers in California to provide consumer credit reporting related services. TU does in fact actually provide such continuous and

ongoing consumer credit reporting related services to such customers in California and has employees in California.

6. Furthermore, this Court has specific personal jurisdiction over TU because the claims in this action stem from its specific contacts with the State of California — namely, TU's provision of consumer credit reporting services to a multitude of customers in California, TU's collection, maintenance, and processing of the personal data of Californians in connection with such services, TU's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent cybersecurity attack and security breach of such data.

7. This Court has federal question jurisdiction subject matter jurisdiction pursuant to 28 U.S.C. § 1331 because this action concerns violation of federal law – the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq*.

8. This Court has diversity subject matter jurisdiction under 28 U.S.C. § 1332(d) in that the mater in controversy exceeds the sum or value of $5,000,000, exclusive of interests and costs, and is a class action in which members of the class defined herein include citizens of a State different from the TU. Specifically, Defendant is a citizen of the state of Delaware and the plaintiff class and/or subclasses defined herein include citizens of other states, including California.

9. Venue is proper in the Northern District of California under 28 U.S.C. § 1391 (b)(1)-(2) and (c)(2) because a substantial part of the events or omissions giving rise to the claims alleged herein occurred within this judicial district, specifically TU's provision of consumer credit reporting related services in California, TU's collection, maintenance, and processing of the personal data of Californians in connection with such services, TU's failure to implement and maintain reasonable security procedures and practices with respect to that data, and the consequent security breach of such data that resulted from TU's failure. In addition, Plaintiff is informed and believes and thereon alleges that members of the class and subclass defined below reside in the Northern District.

INTRADISTRICT ASSIGNMENT

10. Assignment to the San Francisco/Oakland divisions is proper because a substantial part of the events or omissions which give rise to the claims herein occurred within San Francisco County. Further, pursuant to Civil L. R. 3-2(c), all civil actions which arise in the counties of Alameda, Contra Costa, Del Norte, Humboldt, Lake, Marin, Mendocino, Napa, San Francisco, San Mateo, or Sonoma shall be assigned to the San Francisco/Oakland Divisions. A substantial part of the events or omissions giving rise to the claims herein occurred also within these counties and therefore assignment to the San Francisco/Oakland divisions is proper.

FACTUAL BACKGROUND

11. TU is one of the three largest credit bureaus in the world. It collects, stores and maintains a data base of information from more than 1 billion individuals around the world, including more than 200 million active credit users in the United States.

12. TU is a regulated consumer reporting agency. TU is regulated under the Fair Credit Reporting Act ("FCRA") and the California Consumer Credit Reporting Agencies Act.

13. In connection with its work as a credit reporting agency, TU collects, stores, and processes sensitive personal data for millions of individuals in the United States alone. In doing so, TU retains sensitive information including, but not limited to, names, addresses, full Social Security numbers, financial account information and driver's license information.

14. As a corporation doing business in California, TU is legally required to protect personal information from unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction.

15. TU knew that it was a prime target for hackers given the significant amount of sensitive personal information processed through its computer data and storage systems. TU's knowledge is underscored by the massive number of data breaches that have occurred in recent years.

16. Despite knowing the prevalence of data breaches, TU failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. TU has the resources to prevent a breach, but

neglected to adequately invest in data security, despite the growing number of well-publicized breaches. TU failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures as described herein to ensure vulnerabilities were avoided or remedied and that Plaintiff's and class members' data were protected.

17. Specifically, on or around November 7, 2022, TU reported a data breach of its systems. According to TU, an unauthorized actor accessed certain TU files. TU informed impacted individuals that their information was part of the breach. According to TU, the breach resulted in the individuals names, addresses, full Social Security numbers, financial account numbers, and driver's license information being compromised.

18. The data breach impacted approximately 200 million TransUnion customers in the United States.

19. Upon information and belief, the hackers responsible for the data breach stole the personal information of all TU's clients and employees, including Plaintiff's. Because of the nature of the breach and of the personal information stored or processed by TU, Plaintiff is informed and believes that all categories of personal information were further subject to unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction. Plaintiff is informed and believes that criminals would have no purpose for hacking TU other than to exfiltrate or steal, or destroy, use, or modify as part of their ransom attempts, the coveted personal information stored or processed by TU.

20. The personal information exposed by TU as a result of its inadequate data security is highly valuable on the black market to phishers, hackers, identity thieves, and cybercriminals. Stolen personal information is often trafficked on the "dark web," a heavily encrypted part of the Internet that is not accessible via traditional search engines. Law enforcement has difficulty policing the dark web due to this encryption, which allows users and criminals to conceal identities and online activity.

21. When malicious actors infiltrate companies and copy and exfiltrate the personal information that those companies store, or have access to, that stolen information often ends up on the dark web because the malicious actors buy and sell that information for profit.

22. The information compromised in this unauthorized cybersecurity attack involves sensitive personal identifying information, which is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. Whereas here, the information compromised is difficult and highly problematic to change—particularly social security numbers.

23. Once personal information is sold, it is often used to gain access to various areas of the victim's digital life, including bank accounts, social media, credit card, and tax details. This can lead to additional personal information being harvested from the victim, as well as personal information from family, friends, and colleagues of the original victim.

24. Unauthorized data breaches, such as these, facilitate identity theft as hackers obtain consumers' personal information and thereafter use it to siphon money from current accounts, open new accounts in the names of their victims, or sell consumers' personal information to others who do the same.

25. Federal and state governments have established security standards and issued recommendations to minimize unauthorized data disclosures and the resulting harm to individuals and financial institutions. Indeed, the Federal Trade Commission ("FTC") has issued numerous guides for businesses that highlight the importance of reasonable data security practices.

26. According to the FTC, the need for data security should be factored into all business decision-making.[1] In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business.[2] Among other things, the guidelines note businesses should properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection

[1] *See* Federal Trade Commission, Start with Security (June 2015), available at https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited January 27, 2022).

[2] *See* Federal Trade Commission, Protecting Personal Information: A Guide for Business (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited January 27, 2022).

system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of the breach.

27. Also, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[3]

28. Highlighting the importance of protecting against unauthorized data disclosures, the FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect personal information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

29. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

30. The FBI created a technical guidance document for Chief Information Officers and Chief Information Security Officers that compiles already existing federal government and private industry best practices and mitigation strategies to prevent and respond to ransomware attacks. The document is titled *How to Protect Your Networks from Ransomware* and states that on average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016. Yet, there are very effective prevention and response actions that can significantly mitigate the risks.[4] Preventative measure include:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy

[3] *See id.*
[4] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed January 27, 2022).

Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used. Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[5]

31. TU could have prevented the cybersecurity attack by properly utilizing best practices as advised by the federal government, as described in the preceding paragraphs, but failed to do so.

32. TU's failure to safeguard against a cybersecurity attack is exacerbated by the repeated warnings and alerts from public and private institutions, including the federal government, directed to protecting and securing sensitive data. Experts studying cybersecurity routinely identify companies such as TU that collect, process, and store massive amounts of data

[5] *Id.*

on cloud-based systems as being particularly vulnerable to cyberattacks because of the value of the personal information that they collect and maintain. Accordingly, TU knew or should have known that it was a prime target for hackers.

33. According to the 2021 Thales Global Cloud Security Study, more than 40% of organizations experienced a cloud-based data breach in the previous 12 months. Yet, despite these incidents, the study found that nearly 83% of cloud-based businesses still fail to encrypt half of the sensitive data they store in the cloud.[6]

34. Upon information and belief, TU did not encrypt Plaintiff's and class members' personal information involved in the data breach.

35. Despite knowing the prevalence of data breaches, TU failed to prioritize cybersecurity by adopting reasonable security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. TU have the resources to prevent an attack, but neglected to adequately invest in cybersecurity, despite the growing number of well-publicized breaches. TU failed to fully implement each and all of the above-described data security best practices. TU further failed to undertake adequate analyses and testing of its own systems, training of its own personnel, and other data security measures to ensure vulnerabilities were avoided or remedied and that Plaintiff's and class members' data were protected.

Plaintiff's Facts

36. Plaintiff's and class members' personal identifying information, including their names, contact information, financial account numbers, Social Security numbers, driver's license information, among other private personal information, were in the possession, custody and/or control of TU. Plaintiff believed that TU would protect and keep his personal identifying information protected, secure and safe from unlawful disclosure

37. After the data breach, Plaintiff received notice of the data breach from TU via letter.

38. Plaintiff has spent and will continue to spend time and effort monitoring his

[6] Maria Henriquez, *40% of organizations have suffered a cloud-based data breach,* Security, Oct. 29, 2021, https://www.securitymagazine.com/articles/96412-40-of-organizations-have-suffered-a-cloud-based-datq-breach (last visited January 27, 2022).

accounts to protect himself from identity theft. Plaintiff remains concerned for his personal security and the uncertainty of what personal information was exposed to hackers and/or posted to the dark web.

39. As a direct and foreseeable result of TU's negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, Plaintiff and all class members, have suffered harm in that their sensitive personal information has been exposed to cybercriminals and they have an increased stress, risk, and fear of identity theft and fraud. This is not just a generalized anxiety of possible identify theft, privacy, or fraud concerns, but a concrete stress and risk of harm resulting from an actual breach and accompanied by actual instances of reported problems suspected to stem from the breach.

40. Upon information and belief, and as detailed in the November 2022 notice letter, Plaintiff's social security number and other personal information was exfiltrated by the hackers who obtained unauthorized access to his and class members' personal information for unlawful purposes.

41. Social security numbers are among the most sensitive kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an individual's social security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[7]

42. Furthermore, Plaintiff and class members are well aware that their sensitive personal information, including social security numbers and potentially banking information, risks being available to other cybercriminals on the dark web. Accordingly, all Plaintiff and class

[7] *Identify Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited January 27, 2022).

members have suffered harm in the form of increased stress, fear, and risk of identity theft and fraud resulting from the data breach. Additionally, Plaintiff and class members have incurred, and/or will incur, out-of-pocket expenses related to credit monitoring and identify theft prevention to address these concerns.

CLASS ACTION ALLEGATIONS

43. Plaintiff brings this action on behalf of himself and all other similarly situated persons pursuant to Federal Rule of Civil Procedure 23, including Rule 23(b)(1)-(3) and (c)(4). Plaintiff seeks to represent the following class and subclasses:

> **Nationwide Class**. All persons in the United States whose personal information was compromised in or as a result of TU's data breach, which was announced on or around November 7, 2022.
>
> **California Subclass.** All persons residing in California whose personal information was compromised in or as a result of TU's data breach, which was announced on or around November 7, 2022.

Excluded from the class are the following individuals and/or entities: TU and its parents, subsidiaries, affiliates, officers, directors, or employees, and any entity in which TU has a controlling interest; all individuals who make a timely request to be excluded from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

44. Plaintiff reserves the right to amend or modify the class definitions with greater particularity or further division into subclasses or limitation to particular issues.

45. This action has been brought and may be maintained as a class action under Rule 23 because there is a well-defined community of interest in the litigation and the proposed classes are ascertainable, as described further below:

a. Numerosity: The potential members of the class as defined are so numerous that joinder of all members of the class is impracticable. While the precise number of class members at issue has not been determined, Plaintiff believes the cybersecurity breach affected tens of thousands of individuals nationwide and at least many thousands within California.

b. Commonality: There are questions of law and fact common to Plaintiff and the class that predominate over any questions affecting only the individual members of the class. The common questions of law and fact include, but are not limited to, the following:

i. Whether TU owed a duty to Plaintiff and class members to exercise due care in collecting, storing, processing, and safeguarding their personal information;

ii. Whether TU breached those duties;

iii. Whether TU implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information of class members;

iv. Whether TU acted negligently in connection with the monitoring and/or protecting of Plaintiff's and class members' personal information;

v. Whether TU knew or should have known that they did not employ reasonable measures to keep Plaintiff's and class members' personal information secure and prevent loss or misuse of that personal information;

vi. Whether TU adequately addressed and fixed the vulnerabilities which permitted the data breach to occur;

vii. Whether TU caused Plaintiff and class members damages;

viii. Whether the damages TU caused to Plaintiff and class members includes the increased risk and fear of identity theft and fraud resulting from the access and exfiltration, theft, or disclosure of their personal information;

ix. Whether Plaintiff and class members are entitled to credit monitoring and other monetary relief;

x. Whether TU's failure to implement and maintain reasonable security procedures and practices constitutes negligence;

xi. Whether TU's failure to implement and maintain reasonable security procedures and practices constitutes negligence per se;

xii. Whether TU's failure to implement and maintain reasonable security procedures and practices constitutes violation of the Federal Trade Commission Act, 15 U.S.C. § 45(a);

xiii. Whether TU's failure to implement and maintain reasonable security procedures and practices constitutes violation of the Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1681x and California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200; and

xiv. Whether the nationwide class and California subclass are entitled to actual pecuniary damages and/or statutory damages, and the proper measure of such damages.

c. Typicality. The claims of the named Plaintiff are typical of the claims of the class members because all had their personal information compromised as a result of TU's failure to implement and maintain reasonable security measures and the consequent data breach.

d. Adequacy of Representation. Plaintiff will fairly and adequately represent the interests of the class. Counsel who represent Plaintiff are experienced and competent in consumer and employment class actions, as well as various other types of complex and class litigation.

e. Superiority and Manageabilty. A class action is superior to other available means for the fair and efficient adjudication of this controversy. Individual joinder of all Plaintiffs is not practicable, and questions of law and fact common to Plaintiffs predominate over any questions affecting only Plaintiff. Each Plaintiff has been damaged and is entitled to recovery by reason of TU's unlawful failure to adequately safeguard their data. Class action treatment will allow those similarly situated persons to litigate their claims in the manner that is most efficient and economical for the parties and the judicial system. As any civil penalty awarded to any individual class member may be small, the expense and burden of individual litigation make it impracticable for most class members to seek redress

individually. It is also unlikely that any individual consumer would bring an action solely on behalf of himself or herself pursuant to the theories asserted herein. Additionally, the proper measure of civil penalties for each wrongful act will be answered in a consistent and uniform manner. Furthermore, the adjudication of this controversy through a class action will avoid the possibility of inconsistent and potentially conflicting adjudication of the asserted claims. There will be no difficulty in the management of this action as a class action, as TU's records will readily enable the Court and parties to ascertain affected companies and their employees.

46. Class certification is also appropriate under Fed. R. Civ. P. 23(a) and (b)(2) because TU 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.

47. 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 the disposition of the matters and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether TU owed a legal duty to Plaintiff and class members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

b. Whether TU breached that legal duty to Plaintiff and class members to exercise due care in collecting, storing, processing, using, and safeguarding their personal information;

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

d. Whether TU failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information compromised in the breach; and

e. Whether class members are entitled to actual damages, credit monitoring, injunctive relief, statutory damages, and/or punitive damages as a result of TU's wrongful conduct as alleged herein.

FIRST CAUSE OF ACTION
Violation of the Fair Credit Reporting Act,
15 U.S.C. § 1681, *et seq*.
(By Plaintiff and the Nationwide Class Against TU)

48. Plaintiff realleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

49. TU is subject to the Fair Credit Reporting Act because it is a "consumer reporting agency that compiles and maintains files on consumers on a nationwide basis," as outlined in 15 U.S.C. §§ 1681(a)(f) and (p).

50. Plaintiff and members of the class alleged herein are consumers, as defined in 15 U.S.C. § 1681(c).

51. As part of its business as a consumer reporting agency, TU compiles and maintains consumer reports for Plaintiff and members of the class alleged herein, pursuant to 15 U.S.C. § 1681(a)(d).

52. The personal identifying information and other data subject to the data breach of TU's systems announced in November 2022 is a consumer report under the FCRA because it was a communication of information bearing on Plaintiff's and class members' credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, which was anticipated to be used as a factor in obtaining eligibility for credit.

53. Pursuant to 15 U.S.C. § 1681(b)(a), a consumers' credit report can only be used by a CRA for limited purposes and cannot be accesses by unauthorized actors including, but not limited to, hackers and/or participants engaged in a data breach.

54. TU violated 15 U.S.C. § 1681(b)(a) by allowing unauthorized actors to gain access to information contained in Plaintiff's and class members' consumer reports as part of the data breach subject to the instant action.

55. TU failed to maintain, and continues to fail to maintain, procedures, safety and

security measures designed to prevent unauthorized actors from obtaining Plaintiff's and class member's personal identifying information contained in their consumer reports.

56. As a direct and proximate result of TU's failure to implement adequate safety and security measures for Plaintiff's and class members' personal identifying information, TU allowed unauthorized actors to access, remove, exfilrate and otherwise possess, Plaintiff's and class member's consumer reports.

57. TU's unauthorized disclosure of Plaintiff's and class members' consumer reports constitutes a violation of the FCRA, particularly sections 15 U.S.C. § 1681(b) and (e).

58. As a direct and proximate result of TU's negligence, Plaintiff and class members have been injured as described herein, and are entitled to damages, including compensatory, statutory, punitive, and nominal damages, in an amount to be proven at trial. As a result of TU's failure to protect Plaintiff's and class members' personal information, Plaintiff's and class members' personal information has been accessed by malicious cybercriminals.

59. As a direct and proximate result of TU's violation of the FCRA, TU is liable to Plaintiff and members of the class for their actual damages and/or statutory damages, as well as costs and attorney's fees to be proven at trial.

60. TU's failure to comply with the FCRA was willful because TU knew, or should have known, and recklessly disregarded that its cybersecurity measures were inadequate to protect consumers personal identifying information. TU further acted willfully and recklessly because as a consumer reporting agency it should have known of its obligations under the FCRA, and it deprived Plaintiff and class members of their rights under the FCRA.

61. TU is liable to Plaintiff and class members in an amount equal to actual damages, or damages pursuant to statute in the range of not less than $100 and not more than $1,000 for each Plaintiff and member of the class, as well as punitive damages, costs and reasonable attorneys' fees pursuant to 15 U.S.C. § 1681(n)(a).

SECOND CAUSE OF ACTION
Negligence
(By Plaintiff and the Nationwide Class and the California Subclass Against TU)

62. TU owed a duty to Plaintiff and class members to exercise reasonable care in obtaining, storing, using, processing, deleting and safeguarding their personal information in its possession from being compromised, stolen, accessed, and/or misused by unauthorized persons. That duty includes a duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information that were compliant with and/or better than industry-standard practices. TU's duties included a duty to design, maintain, and test its security systems to ensure that Plaintiff's and class members' personal information was adequately secured and protected, to implement processes that would detect a breach of its security system in a timely manner, to timely act upon warnings and alerts, including those generated by its own security systems regarding intrusions to its networks, and to promptly, properly, and fully notify its customers, Plaintiff, and class members of any data breach.

63. TU's duties to use reasonable care arose from several sources, including but not limited to those described below.

64. TU had a common law duty to prevent foreseeable harm to others. This duty existed because Plaintiff and class members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiff and class members would be harmed by the failure to protect their personal information because hackers routinely attempt to steal such information and use it for nefarious purposes, but TU also knew that it was more likely than not Plaintiff and other class members would be harmed.

65. TU's duty also arose under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as TU.

66. Various FTC publications and data security breach orders further form the basis of TU's duty. According to the FTC, the need for data security should be factored into all business

decision making.[8] In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.[9] Among other things, the guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach. Additionally, the FTC recommends that companies limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures. The FBI has also issued guidance on best practices with respect to data security that also form the basis of TU's duty of care, as described above.[10]

67. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and class members' personal information, TU assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and class members' personal information from disclosure.

68. TU also had a duty to safeguard the personal information of Plaintiff and class members and to promptly notify them of a breach because of state laws and statutes that require TU to reasonably safeguard personal information, as detailed herein.

69. TU also had a duty based on the FCRA and as a consumer credit agency to protect

[8] *Start with Security, A Guide for Business*, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

[9] *Protecting Personal Information, A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf

[10] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed January 27, 2022).

Plaintiff's and members of the class' personal identifying information for unauthorized disclosure.

70. Timely notification was required, appropriate, and necessary so that, among other things, Plaintiff and class members could take appropriate measures to freeze or lock their credit profiles, cancel or change usernames or passwords on compromised accounts, monitor their account information and credit reports for fraudulent activity, contact their banks or other financial institutions that issue their credit or debit cards, obtain credit monitoring services, develop alternative timekeeping methods or other tacks to avoid untimely or inaccurate wage payments, and take other steps to mitigate or ameliorate the damages caused by TU's misconduct.

71. Plaintiff and class members have taken reasonable steps to maintain the confidentiality of their personal information.

72. TU breached the duties it owed to Plaintiff and class members described above and thus was negligent. TU breached these duties by, among other things, failing to: (a) exercise reasonable care and implement adequate security systems, protocols and practices sufficient to protect the personal information of Plaintiff and class members; (b) prevent the breach; (c) timely detect the breach; (d) maintain security systems consistent with industry; (e) timely disclose that Plaintiff's and class members' personal information in TU's possession had been or was reasonably believed to have been stolen or compromised; (f) failing to comply fully even with its own purported security practices.

73. TU knew or should have known of the risks of collecting and storing personal information and the importance of maintaining secure systems, especially in light of the increasing frequency of ransomware attacks. The sheer scope of TU's operations further shows that TU knew or should have known of the risks and possible harm that could result from its failure to implement and maintain reasonable security measures. On information and belief, this is but one of the several vulnerabilities that plagued TU's systems and led to the data breach.

74. Through TU's acts and omissions described in this complaint, including TU's failure to provide adequate security and its failure to protect the personal information of Plaintiff and class members from being foreseeably captured, accessed, exfiltrated, stolen, disclosed,

accessed, and misused, TU unlawfully breached their duty to use reasonable care to adequately protect and secure Plaintiff's and class members' personal information.

75. TU further failed to timely and accurately disclose to customers, Plaintiff, and class members that their personal information had been improperly acquired or accessed and/or was available for sale to criminals on the dark web. TU has not provided a data breach notice to the Attorney General of California, which would provide statewide notice to impacted individuals. Plaintiff and class members could have taken action to protect their personal information if they were provided timely notice.

76. But for TU's wrongful and negligent breach of its duties owed to Plaintiff and class members, their personal information would not have been compromised.

77. Plaintiff and class members relied on TU to keep their personal information confidential and securely maintained, and to use this information for business purposes only, and to make only authorized disclosures of this information.

78. As a direct and proximate result of TU's negligence, Plaintiff and class members have been injured as described herein, and are entitled to damages, including compensatory, punitive, and nominal damages, in an amount to be proven at trial. As a result of TU's failure to protect Plaintiff's and class members' personal information, Plaintiff's and class members' personal information has been accessed by malicious cybercriminals. Plaintiff's and the class members' injuries include:

a. theft of their personal information;

b. costs associated with requested credit freezes;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. costs associated with purchasing credit monitoring and identity theft protection services;

e. unauthorized charges and loss of use of and access to their financial account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their

accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit;

f. lowered credit scores resulting from credit inquiries following fraudulent activities;

g. costs associated with time spent and loss of productivity from taking time to address and attempt to ameliorate, mitigate, and deal with the actual and future consequences of the data breach, including finding fraudulent charges, cancelling and reissuing cards, enrolling in credit monitoring and identity theft protection services, freezing and unfreezing accounts, and imposing withdrawal and purchase limits on compromised accounts;

h. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their personal information being placed in the hands of criminals;

i. damages to and diminution of value of their personal information entrusted, directly or indirectly, to TU with the mutual understanding that TU would safeguard Plaintiff's and the class members' data against theft and not allow access and misuse of their data by others;

j. continued risk of exposure to hackers and thieves of their personal information, which remains in TU's possession and is subject to further breaches so long as TU fails to undertake appropriate and adequate measures to protect Plaintiff and class members, along with damages stemming from the stress, fear, and anxiety of an increased risk of identity theft and fraud stemming from the breach;

k. loss of the inherent value of their personal information;

l. the loss of the opportunity to determine for themselves how their personal information is used; and

m. other significant additional risk of identity theft, financial fraud, and other identity-related fraud in the indefinite future.

79. In connection with the conduct descried above, TU acted wantonly, recklessly, and

with complete disregard for the consequences Plaintiff and class members would suffer if their highly sensitive and confidential personal information, including but not limited to name, company name, address, Social Security numbers, and banking, financial and credit card information, among other sensitive information, was access by unauthorized third parties.

THIRD CAUSE OF ACTION
Negligence Per Se
(By Plaintiff and the Nationwide Class and the California Subclass Against TU)

80. Plaintiff realleges and incorporates by reference the preceding paragraphs as if fully set forth herein.

81. Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect personal information by companies such as TU. Various FTC publications and data security breach orders further form the basis of TU's duty. In addition, individual states have enacted statutes based on the FTC Act that also created a duty.

82. TU violated Section 5 of the FTC Act by failing to use reasonable measures to protect personal information and not complying with industry standards. TU's conduct was particularly unreasonable given the nature and amount of personal information it obtained and stored and the foreseeable consequences of a data breach.

83. TU's violation of Section 5 of the FTC Act constitutes negligence *per se*.

84. Plaintiff and class members are consumers within the class of persons Section 5 of the FTC Act was meant to protect.

85. Moreover, the harm that has occurred is the type of harm that the FTC Act was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the class.

86. As a direct and proximate result of TU's negligence, Plaintiff and class members have been injured as described herein, and are entitled to damages, including compensatory,

punitive, and nominal damages, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
Declaratory Judgment
(By Plaintiff and the Nationwide Class and the California Subclass Against TU)

87. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

88. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201 *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this complaint.

89. An actual controversy has arisen in the wake of the TU data breach regarding its present and prospective common law and other duties to reasonably safeguard consumers personal identifying information in its possession, custody and/or control and regarding whether TU is currently maintaining data security measures adequate to protect Plaintiff and class members from further data breaches that compromise their personal information. Plaintiff alleges that TU's data security measures remain inadequate. TU denies these allegations. Plaintiff continues to suffer injury as a result of the compromise of his personal information and remains at imminent risk that further compromises of her personal information will occur in the future.

90. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. TU continues to owe a legal duty to secure consumers' personal information, including Plaintiff's and class members' personal information, to timely notify them of a data breach under the common law, Section 5 of the FTC Act; and

b. TU continues to breach this legal duty by failing to employ reasonable measures to secure Plaintiff's and class members' personal information.

91. The Court should issue corresponding prospective injunctive relief requiring TU to employ adequate security protocols consistent with law and industry standards to protect Plaintiff's and class members' personal information.

92. If an injunction is not issued, Plaintiff will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at TU. The risk of another such breach is real, immediate, and substantial. If another breach at TU occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

93. The hardship to Plaintiff if an injunction does not issue exceeds the hardship to TU if an injunction is issued. Among other things, if another massive data breach occurs, Plaintiff and class members will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to TU of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and TU has a pre-existing legal obligation to employ such measures.

94. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach, thus eliminating the additional injuries that would result to Plaintiff and the thousands of class members whose confidential information would be further compromised.

FIFTH CAUSE OF ACTION
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code §17200 *et seq.*
(By Plaintiff and the California Subclass Against TU)

95. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

96. TU is a "person" defined by Cal. Bus. & Prof. Code § 17201.

97. TU violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

98. TU' "unfair" acts and practices include:

a. TU failed to implement and maintain reasonable security measures to protect Plaintiff's and California sublcass members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the TU data breach. TU failed to identify foreseeable security

risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents and known coding vulnerabilities in the industry;

b. TU's failure to implement and maintain reasonable security measures also was contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act (15 U.S.C. § 45), California's Customer Records Act (Cal. Civ. Code § 1798.80 *et seq.*), and California's Consumer Privacy Act (Cal. Civ. Code § 1798.150);

c. TU's failure to implement and maintain reasonable security measures also led to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of TU's inadequate security, consumers could not have reasonably avoided the harms that TU caused; and

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

99. TU has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law.

100. TU's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff's and California subclass members' personal information, which was a direct and proximate cause of the TU data breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the TU data breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80 *et seq.*, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150, which was a direct and proximate cause of the TU data breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's and California subclass members' personal information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150;

f. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff's and California subclass members' personal information; and

g. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and California subclass members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, California's Customer Records Act, Cal. Civ. Code §§ 1798.80, *et seq*., and California's Consumer Privacy Act, Cal. Civ. Code § 1798.150.

101. TU's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of TU's data security and ability to protect the confidentiality of consumers' personal information.

102. As a direct and proximate result of TU's unfair, unlawful, and fraudulent acts and practices, Plaintiff and California subclass members were injured and lost money or property,

which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein, monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

103. TU's violations were, and are, willful, deceptive, unfair, and unconscionable.

104. Plaintiff and class members have lost money and property as a result of TU's conduct in violation of the UCL, as stated herein and above.

105. By deceptively storing, collecting, and disclosing their personal information, TU has taken money or property form Plaintiff and class members.

106. TU acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiff's and California subclass members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

107. Plaintiff and California subclass members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from TU's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

SIXTH CAUSE OF ACTION
Invasion of Privacy
(Count 1 – Common Law Invasion of Privacy – Intrusion Upon Seclusion
By Plaintiff and the California Subclass Against TU)

108. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

109. To assert claims for intrusion upon seclusion, one must plead (1) that the defendant intentionally intruded into a matter as to which plaintiff had a reasonable expectation of privacy; and (2) that the intrusion was highly offensive to a reasonable person.

110. TU intentionally intruded upon the solitude, seclusion and private affairs of Plaintiff and class members by intentionally configuring their systems in such a way that left them vulnerable to malware/ransomware attack, thus permitting unauthorized access to their

systems, which compromised Plaintiff's and class members' personal information. Only TU had control over its systems.

111. TU's conduct is especially egregious and offensive as they failed to have adequate security measures in place to prevent, track, or detect in a timely fashion unauthorized access to Plaintiff's and class members' personal information.

112. At all times, TU was aware that Plaintiff's and class members' personal information in their possession contained highly sensitive and confidential personal information.

113. Plaintiff and class members have a reasonable expectation of privacy in their personal information, which also contains highly sensitive medical information.

114. TU intentionally configured their systems in such a way that stored Plaintiff's and class members' personal information to be left vulnerable to malware/ransomware attack without regard for Plaintiff's and class members' privacy interests.

115. The disclosure of the sensitive and confidential personal information of thousands of consumers, was highly offensive to Plaintiff and class members because it violated expectations of privacy that have been established by general social norms, including by granting access to information and data that is private and would not otherwise be disclosed.

116. TU's conduct would be highly offensive to a reasonable person in that it violated statutory and regulatory protections designed to protect highly sensitive information, in addition to social norms. TU's conduct would be especially egregious to a reasonable person as TU publicly disclosed Plaintiff's and class members' sensitive and confidential personal information without their consent, to an "unauthorized person," i.e., hackers.

117. As a result of TU's actions, Plaintiff and class members have suffered harm and injury, including but not limited to an invasion of their privacy rights.

118. Plaintiff and class members have been damaged as a direct and proximate result of TU's intrusion upon seclusion and are entitled to just compensation.

119. Plaintiff and class members are entitled to appropriate relief, including compensatory damages for the harm to their privacy, loss of valuable rights and protections, and heightened stress, fear, anxiety and risk of future invasions of privacy.

(Count 2 –Invasion of Privacy – Cal. Const. Art. 1, § 1
By Plaintiff and the California Subclass Against TU)

120. Plaintiff realleges and incorporates by reference the preceding paragraphs as though fully set forth herein.

121. Art. I, § 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Art. I, § 1, Cal. Const.

122. The right to privacy in California's constitution creates a private right of action against private and government entities.

123. To state a claim for invasion of privacy under the California Constitution, a plaintiff must establish: (1) a legally protected privacy interest; (2) a reasonable expectation of privacy; and (3) an intrusion so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

124. TU violated Plaintiff's and class members' constitutional right to privacy by collecting, storing, and disclosing their personal information in which they had a legally protected privacy interest, and in which they had a reasonable expectation of privacy in, in a manner that was highly offensive to Plaintiff and class members, would be highly offensive to a reasonable person, and was an egregious violation of social norms.

125. TU has intruded upon Plaintiff's and class members' legally protected privacy interests, including interests in precluding the dissemination or misuse of their confidential personal information.

126. TU's actions constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the invasion occurred within a zone of privacy protected by the California Constitution, namely the misuse of information gathered for an improper purpose; and (ii) the invasion deprived Plaintiff and class members of the ability to control the circulation of their personal information, which is considered fundamental to the right to privacy.

127. Plaintiff and class members had a reasonable expectation of privacy in that: (i) TU's invasion of privacy occurred as a result of TU's security practices including the collecting, storage, and unauthorized disclosure of consumers' personal information; (ii) Plaintiff and class members did not consent or otherwise authorize TU to disclosure their personal information; and (iii) Plaintiff and class members could not reasonably expect TU would commit acts in violation of laws protecting privacy.

128. As a result of TU's actions, Plaintiff and class members have been damaged as a direct and proximate result of TU's invasion of their privacy and are entitled to just compensation.

129. Plaintiff and class members suffered actual and concrete injury as a result of TU's violations of their privacy interests. Plaintiff and class members are entitled to appropriate relief, including damages to compensate them for the harm to their privacy interests, loss of valuable rights and protections, heightened stress, fear, anxiety, and risk of future invasions of privacy, and the mental and emotional distress and harm to human dignity interests caused by Defendant's invasions.

130. Plaintiff and class members seek appropriate relief for that injury, including but not limited to damages that will reasonably compensate Plaintiff and class members for the harm to their privacy interests as well as disgorgement of profits made by TU as a result of its intrusions upon Plaintiff's and class members' privacy.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself, the nationwide class, and the California subclass, prays for the following relief:

1. An order certifying the nationwide class and California subclass as defined above pursuant to Fed. R. Civ. P. 23 and declaring that Plaintiff is proper class representative and appointing Plaintiff's counsel as class counsel;
2. Permanent injunctive relief to prohibit TU from continuing to engage in the unlawful acts, omissions, and practices described herein;
3. Compensatory, consequential, general, and nominal damages in an amount to be

proven at trial, in excess of $5,000,000;

4. Disgorgement and restitution of all earnings, profits, compensation, and benefits received as a result of the unlawful acts, omissions, and practices described herein;
5. Punitive, exemplary, and/or trebled damages to the extent permitted by law;
6. Statutory damages pursuant to 15 U.S.C. § 1681(n)(a);
7. A declaration of right and liabilities of the parties;
8. Costs of suit;
9. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code § 1021.5;
10. Pre- and post-judgment interest at the maximum legal rate;
11. Distribution of any monies recovered on behalf of members of the class or the general public via fluid recovery or *cy pres* recovery where necessary and as applicable to prevent Defendant from retaining the benefits of their wrongful conduct; and
12. Such other relief as the Court deems just and proper.

Dated: February 8, 2023

WUCETICH & KOROVILAS LLP

By: /s/ Jason M. Wucetich
JASON M. WUCETICH
Attorneys for Plaintiff
JUDE OKPALA,
individually and on behalf of
all others similarly situated

DEMAND FOR JURY TRIAL

Plaintiff, on behalf of himself and the putative class and subclass, hereby demands a trial by jury on all issues of fact or law so triable.

Dated: February 8, 2023

WUCETICH & KOROVILAS LLP

By: /s/ Jason M. Wucetich
JASON M. WUCETICH
Attorneys for Plaintiff
JUDE OKPALA,
individually and on behalf of
all others similarly situated