Proof

Serve Documents

MIPS Holding, Inc.

Primary Address

2710 Gateway Oaks Drive, Sacramento, CA 95833

Serve By
4 attempts by October 19th

Speed
Standard

Servee Information

Type	Entity
Name	MIPS Holding, Inc.
Registered Agent	CSC - Lawyers Incorporating Service
Primary Address	Residential - 2710 Gateway Oaks Drive, Sacramento, CA 95833
Physical Description	None
Additional Notes	None

Job Information

Job Number:	693846
Matter Number/Name	
Witness Fee	None
Subpoena	No
Related to an Eviction	No
Linked Job(s)?	No

Documents List

1. Complaint
2. Civil Cover Sheet
3. Civil Lawsuit Notice
4. Summons

Client Specifications

None	None

MIPS Holding, Inc.

Primary Address
2710 Gateway Oaks Drive, Sacramento, CA 95833

Attempt Log

Date	Description

California Serve Rules

Notary
Not Required

Civil Subpoenas must be personally served (no sub service)

Can serve on Sundays

BUSINESS ENTITIES (INC., LLC, ETC.)
+ Registered agent + President, Vice President, CEO, or other head of the corporation, a secretary or assistant secretary, a treasurer or assistant treasurer, a controller or chief financial officer, a general manager. (If a bank, to a cashier or assistant cashier) + If none of the persons above are available at the time of attempted service, leaving the documents with the person apparently in charge of the office or the mailing address of one of the persons above and mailing a copy of the summons and complaint to this person at the address where the documents are left.

PUBLIC ENTITY (STATE, COUNTY, CITY, ETC.)
+ Clerk, secretary, president, presiding officer, or other head of its governing body. + If none of the above available, handing to person apparently in charge of the office and mailing a copy of the summons and complaint to one of the individuals in bullet above

MINOR OR INCOMPETENT PERSON
+ Parent, guardian or conservator - if no such person can be found, any person having the care or control of such minor at their house or work + COPY to the minor/individual if they are 12+

POSTING(EVICTIONS)
+ Mail copies must be followed after posting - Must include affidavit showing the time and place of posting + Must mail to tenant, subtenant, and any occupants - Must include affidavit showing the time and place copies of the summons and of the complaint were mailed

INDIVIDUAL
+ Personal + Substituted (MUST HAVE ATTEMPTED TO PERSONALLY SERVE 3 TIMES PRIOR TO SUB SERVICE ON FOURTH ATTEMPT) + Dwelling/house/Usual place of abode - competent member of the household, 18+ - be informed of the contents thereof - Must also mail copy to the place where a copy of the summons and complaint were left + Usual place of business - person apparently in charge, 18+ - be informed of the contents thereof - Must also mail copy at the place where a copy of the summons and complaint were left + Usual mailing address - person apparently in charge, 18+ - be informed of the contents thereof - Must also mail copy at the place where a copy of the summons and complaint were left

Andrew G. Gunem (SBN 354042)
Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borrelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
980 N. Michigan Avenue, Suite 1610
Chicago, Illinois 60611
Telephone: (872) 263-1100
Facsimile: (872) 263-1109
agunem@straussborrelli.com
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for the Plaintiff

SUPERIOR COURT OF THE STATE OF CALIFORNIA
FOR THE COUNTY OF SANTA CLARA

RAJ KUMAR SINGH PARIHAR, on behalf of himself and all others similarly situated,

Plaintiff,

v.

MIPS HOLDING, INC.,

Defendant.

Case No. 24CV448267

DEMAND FOR JURY TRIAL

CLASS ACTION COMPLAINT

Plaintiff Raj Kumar Singh Parihar ("Plaintiff") brings this Class Action Complaint ("Complaint") against Defendant MIPS HOLDING, INC., ("MIPS" or "Defendant") individually, on behalf of all others similarly situated, and alleges, upon personal knowledge as to his own actions and his counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This Class Action arises from a recent cyberattack resulting in a data breach of sensitive information in the possession and custody and/or control of Defendant (the "Data Breach").

2. The Data Breach resulted in unauthorized disclosure, exfiltration, and theft of current and former employees' highly personal information, including first and last names and Social Security Numbers ("personally identifying information" or "PII").

3. On information and belief, on June 26, 2024 MIPS became aware that a Data Breach had occurred on June 26, 2024. However, due to intentionally obfuscating language, it is unclear precisely how long the cybercriminals had access to Defendant's network.

4. On or around September 18, 2024–two months after the Data Breach first occurred–MIPS finally began notifying Class Members about the Data Breach ("Breach Notice"). A copy of Plaintiff's Breach Notice is attached as Exhibit A.

5. MIPS took two months before informing Class Members even though Plaintiff and thousands of Class Members had their most sensitive personal information accessed, exfiltrated, and stolen, causing them to suffer ascertainable losses in the form of the loss of the benefit of their bargain and the value of their time reasonably incurred to remedy or mitigate the effects of the attack.

6. MIPS' Breach Notice obfuscated the nature of the breach and the threat it posted—refusing to tell its employees how many people were impacted, how the breach happened, how long the cybercriminals had access to Defendant's network, and why it took Defendant until September 18, 2024, to begin notifying victims that hackers had gained access to highly sensitive PII.

7. Defendant's failure to timely detect and report the Data Breach made its employees vulnerable to identity theft without any warnings to monitor their financial accounts or credit reports to prevent unauthorized use of their PII.

8. Defendant knew or should have known that each victim of the Data Breach deserved prompt and efficient notice of the Data Breach and assistance in mitigating the effects of PII misuse.

9. In failing to adequately protect Plaintiff's and the Class's PII, failing to adequately notify them about the breach, and by obfuscating the nature of the breach, Defendant violated state and federal law and harmed an unknown number of its current and former employees.

10. Plaintiff and members of the proposed Class are victims of Defendant's negligence and inadequate cyber security measures. Specifically, Plaintiff and members of the proposed Class trusted Defendant with their PII. But Defendant betrayed that trust. Defendant failed to properly use up-to-date security practices to prevent the Data Breach.

11. Plaintiff is a Data Breach victim.

12. Accordingly, Plaintiff, on behalf of himself and a class of similarly situated individuals, brings this lawsuit seeking injunctive relief, damages, and restitution, together with costs and reasonable attorneys' fees, the calculation of which will be based on information in Defendant's possession.

PARTIES

13. Plaintiff, Raj Kumar Singh Parihar is a natural person and citizen of California, where he intends to remain. He was formerly employed at MIPS and is a Data Breach victim.

14. Defendant, MIPS Holding, Inc., is a Stock Corporation formed in Delaware, with its principal place of business at 780 Montague Expressway, Suite 308, San Jose, California 95131.

JURISDICTION AND VENUE

15. This Court has jurisdiction over this action under California Code of Civil Procedure § 410.10. The total amount of damages incurred by Plaintiff and the Class in the aggregate exceeds the $35,000 jurisdictional minimum of this Court. Upon information and belief, more than two-thirds of the proposed Class are citizens and residents of California.

16. Venue is proper in this Court under California Bus. & Prof. Code § 17203 and Code of Civil Procedure §§ 395(a) and 395.5 because Defendant is headquartered in this judicial district and a substantial part of the events or omissions giving rise to Plaintiff's claims occurred in this judicial district.

STATEMENT OF FACTS

MIPS

17. MIPS is computer IP company that "designs efficient and configurable compute Cores for automotive, data center and embedded systems."[1] Defendant's website boasts that "MIPS-based chips can be found in billions of devices and systems around the world."[2]

18. As part of its business, MIPS receives and maintains the PII of hundreds of current and former employees. In doing so, MIPS implicitly promises to safeguard their PII.

[1] About, MIPS, https://mips.com/company/# (last visited September 26, 2024).
[2] *Id.*

19. In collecting and maintaining its current and former employees' PII, MIPS agreed it would safeguard the data in accordance with state law, and federal law. After all, Plaintiff and Class Members themselves took reasonable steps to secure their PII.

20. Despite recognizing its duty to do so, on information and belief, MIPS has not implemented reasonably cybersecurity safeguards or policies to protect its employees' PII or supervised its IT or data security agents and employees to prevent, detect, and stop breaches of its systems. As a result, MIPS leaves significant vulnerabilities in its systems for cybercriminals to exploit and gain access to employees' PII.

The Data Breach

21. Plaintiff is a former employee of MIPS. As a condition of employment with Defendant, it requires its employees to disclose PII including but not limited to, their first and last names and Social Security numbers. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

22. On information and belief, Defendant collects and maintains current and former employees' PII in its computer systems.

23. In collecting and maintaining PII, Defendant implicitly agrees that it will safeguard the data using reasonable means according to state and federal law.

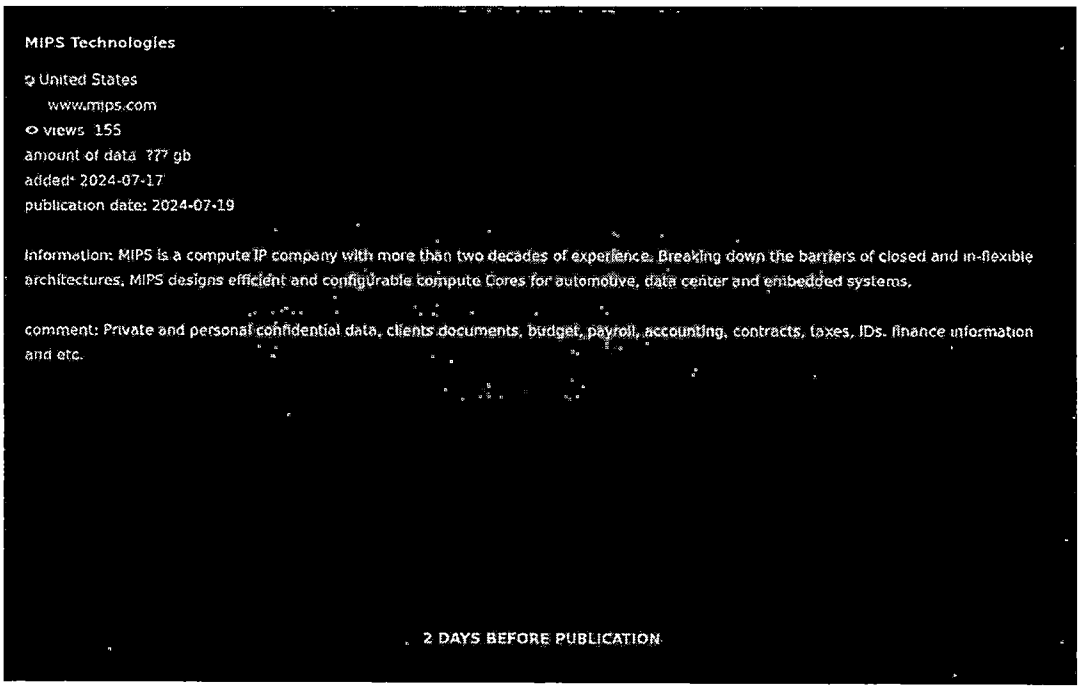
24. According to the Breach notice, "[o]n June 26, 2024, we became aware of suspicious activity occurring within our network." Ex. A.

25. Following an investigation, Defendant "determined that there was unauthorized access to our network and that certain files and folders were viewed and/or acquired by an unknown actor on June 26, 2024." Ex. A.

26. In other words, Defendant's cyber and data security systems were completely inadequate in that it allowed cybercriminals to obtain files containing a treasure trove of thousands of its employees' highly sensitive PII.

27. Through its inadequate security practices, Defendant exposed Plaintiff's and the Class's PII for theft and sale on the dark web.

28. Since the Data Breach occurred, the notorious cybercriminal group "Play" has claimed responsibility for the attack.[3]



29. Thus far, Play has:

a. claimed to have accessed and stolen data from Defendant— including highly sensitive PII;

b. and has threatened to *publish the data* if a ransom is not paid.[4]

[3] https://www.ransomlook.io/screenshots/play/MIPS%20Technologies.png (last visited September 26, 2024).
[4] *Id.*

30. Play's post indicates that the sensitive data that they exfiltrated includes "private and personal confidential information, client documents, budget, payroll, accounting, contracts, taxes, IDs, finance information and etc."[5]

31. The day prior to the publication of the stolen data, Play's post indicated that it had been viewed at least 330 times.[6]

Victim Name	**MIPS Technologies**
Victim Website *(if available)*	**www[.]mips[.]com**
Victim Country	**United States**
Date Added	**2024-07-17**
Publication Date(of files)	**2024-07-19**
Dark Web Post Views	**330**
Publication Status	**1 DAY BEFORE PUBLICATION**

32. Further, Play threatened to publish the stolen data if the ransom was not paid by July 19, 2024.[7]

33. Thus, upon information and belief, Plaintiff and the Class' information has already been published on the dark web.

34. Play is a particularly sophisticated and dangerous criminal group, having "evolved from data theft to using ransomware tactics."[8]

35. Play has been profiled by the Federal Bureau of Investigation (FBI) and

---

[5] *Id.*
[6] https://www.hookphish.com/blog/ransomware-play-group-hits-mips-technologies/ (last visited September 26, 2024).
[7] https://www.ransomlook.io/screenshots/play/MIPS%20Technologies.png (last visited September 26, 2024).
[8] https://ransomwareattacks.halcyon.ai/attacks/fpl-food-llc-targeted-by-play-ransomware-group (last visited September 26, 2024).

the Cybersecurity and Infrastructure Security Agency (CISA).[9] In a joint advisory, these federal agencies issued the following warnings about Play:

a. "Since June 2022, the Play (also known as Playcrypt) ransomware group has impacted a wide range of businesses and critical infrastructure in North America, South America, and Europe;"

b. "As of October 2023, the FBI was aware of approximately 300 affected entities allegedly exploited by [Play];"

c. "Play ransomware group is presumed to be a closed group, designed to 'guarantee the secrecy of deals,' according to a statement on the group's data leak website;"

d. "Play ransomware actors employ a double-extortion model, encrypting systems after exfiltrating data. Ransom notes do not include an initial ransom demand or payment instructions, rather, victims are instructed to contact the threat actors via email."[10]

36. Employees place value in data privacy and security. These are important considerations when deciding who to work and provide services for. Plaintiff would not have accepted the Defendant's employment offer, nor provided his PII, to Defendant had they known that MIPS does not take all necessary precautions to secure the PII given to it by its employees.

37. On or around September 18, 2024 –two months after the Breach was discovered– Defendant finally notified Plaintiff and Class Members about the Data Breach.

[9] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a (last visited September 26, 2024).

[10] *Id.*

38. Despite its duties and alleged commitments to safeguard PII, Defendant did not in fact follow industry standard practices in securing its employees' PII, as evidenced by the Data Breach.

39. In response to the Data Breach, Defendant contends that it would "continue to implement technical security measures to strengthen the security of [its] systems." Ex. A. Although Defendant fails to expand on what these alleged "measures" are, such measures should have been in place before the Data Breach.

40. Through its Breach Notice, Defendant also recognized the actual imminent harm and injury that flowed from the Data Breach, so it encouraged breach victims to "remain vigilant against incidents of identity theft or fraud and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." Ex. A.

41. Defendant also recognized through its Breach Notice, its duty to implement reasonable cybersecurity safeguards and policies to protect its employees' PII, insisting that, "[t]he privacy and security of information in our possession is one of our highest priorities." Ex. A.

42. Cybercriminals need not harvest a person's Social Security number or financial account information in order to commit identity fraud or misuse Plaintiff's and the Class's PII. Cybercriminals can cross-reference the data stolen from the Data Breach and combine with other sources to create "Fullz" packages, which can then be used to commit fraudulent account activity on Plaintiff's and the Class's financial accounts.

43. On information and belief, MIPS has offered several months of complimentary credit monitoring services to victims, which does not adequately address the lifelong harm that

victims will face following the Data Breach. Indeed, the breach involves PII that cannot be changed, such as Social Security numbers.

44. Even with several months' worth of credit monitoring services, the risk of identity theft and unauthorized use of Plaintiff's and Class Members' PII is still substantially high. The fraudulent activity resulting from the Data Breach may not come to light for years.

45. On information and belief, Defendant failed to adequately train and supervise its IT and data security agents and employees on reasonable cybersecurity protocols or implement reasonable security measures, causing it to lose control over its employees' PII. Defendant's negligence is evidenced by its failure to prevent the Data Breach and stop cybercriminals from accessing the PII.

The Data Breach was a Foreseeable Risk of which Defendant was on Notice.

46. Defendant's data security obligations were particularly important given the substantial

47. Defendant's data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches in the manufacturing industry preceding the date of the breach.

48. In light of recent high profile data breaches at other manufacturing companies, Defendant knew or should have known that its electronic records and employees' PII would be targeted by cybercriminals.

49. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020. The 330 reported breaches reported in 2021 exposed nearly 30 million sensitive records (28,045,658),

compared to only 306 breaches that exposed nearly 10 million sensitive records (9,700,238) in 2020.

50. Indeed, cyberattacks have become increasingly common for over ten years, with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cybercrime."

51. Cyberattacks on manufacturing companies like Defendant have become extremely notorious in recent years, with manufacturing firms suffering more than 130 data breaches, exposed 38 million records, in 2022. Further, "since 2020, US businesses that specialize in manufacturing and utilities have suffered 973 data breaches affecting more than 202 million records."

52. Therefore, the increase in such attacks, and attendant risk of future attacks, was widely known to the public and to anyone in Defendant's industry, including Defendant.

Plaintiff Raj's Experience

53. Plaintiff was a MIPS employee between 2014-2016 and is a Data Breach victim.

54. As a condition of employment with Defendant, MIPS required Plaintiff to disclose his PII. Defendant used that PII to facilitate its employment of Plaintiff, including payroll, and required Plaintiff to provide that PII to obtain employment and payment for that employment.

55. Plaintiff provided his PII to Defendant and trusted that it would use reasonable measures to protect it according to state and federal law.

56. Defendant deprived Plaintiff of the earliest opportunity to guard himself against the Data Breach's effects by failing to notify him about it for two months.

57. As a result of its inadequate cybersecurity, Defendant exposed Plaintiff's PII for theft by cybercriminals and sale on the dark web.

58. As a result of the Data Breach notice, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring his accounts and credit reports to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

59. Plaintiff has and will spend considerable time and effort monitoring his accounts to protect himself from additional identity theft. Plaintiff fears for his personal financial security and uncertainty over what PII was exposed in the Data Breach.

60. Plaintiff has and is experiencing feelings of anxiety, sleep disruption, stress, fear, and frustration because of the Data Breach. This goes far beyond allegations of mere worry or inconvenience; it is exactly the sort of injury and harm to a Data Breach victim that the law contemplates and addresses.

61. Plaintiff has suffered actual injury in the form of damages to and diminution in the value of his PII —a form of intangible property that Plaintiff entrusted to Defendant, which was compromised in and as a result of the Data Breach.

62. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII being placed in the hands of unauthorized third parties and possibly criminals.

63. Indeed, following the Data Breach, Plaintiff began experiencing a substantial increase in spam and scam phone calls regarding loans and financing, suggesting that his PII has been placed in the hands of cybercriminals.

64. On information and belief, Plaintiff's phone number was compromised as a result of the Data Breach, as cybercriminals are able to use an individual's PII that is accessible on the dark web, as Plaintiff's is here, to gather and steal even more information.

65. Once an individual's PII is for sale and access on the dark web, as Plaintiff's PII is here as a result of the Breach, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[11]

66. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendant's possession, is protected, and safeguarded from future breaches.

Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft

67. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

68. As a result of Defendant's failure to prevent the Data Breach, Plaintiff and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

[11] What do Hackers do with Stolen Information, Aura, https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited September 26, 2024).

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in Defendant's possession and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII in its possession.

69. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to $1,000.00 depending on the type of information obtained.

70. The value of Plaintiff's and the Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen PII openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

71. It can take victims years to spot identity theft, giving criminals plenty of time to use that information for cash.

72. One such example of criminals using PII for profit is the development of "Fullz" packages.

73. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and

degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as "Fullz" packages.

74. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff and the proposed Class's phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiff and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff's and the Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

75. Defendant disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

76. Defendant's failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff's and the Class's injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

Defendant failed to adhere to FTC guidelines.

77. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

78. 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. The guidelines explain that businesses should:

a. protect the sensitive consumer information that it keeps;

b. properly dispose of PII that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

79. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

80. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; 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.

81. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, 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 ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

82. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's PIIconstitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

Defendant Fails to Comply with Industry Standards

83. As noted above, experts studying cyber security routinely identify entities in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

84. Several best practices have been identified that a minimum should be implemented by employers in possession of PII, like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendant failed to follow these industry best practices, including a failure to implement multi-factor authentication.

85. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendant failed to follow these cybersecurity best practices, including failure to train staff.

86. Upon information and belief, Defendant failed to implement industry-standard cybersecurity measures, including failing to meet the minimum standards of both the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04).

87. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendant failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

88. Plaintiff, on behalf of himself, and all others similarly situated pursuant to California's Class Action Mechanism (Cal. Civ., § 382) for the following Class defined as:

> All individuals residing in the United States whose PII was compromised in the Data Breach, including all those who received notice of the breach.

89. Excluded from the Class is Defendant, their agents, affiliates, parents, subsidiaries, any entity in which Defendant have a controlling interest, any of Defendant's officers or directors, any successors, and any Judge who adjudicates this case, including their staff and immediate family.

90. Plaintiff reserves the right to amend the class definition.

91. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of his claims on class-wide bases using the same

evidence as would be used to prove those elements in individual actions asserting the same claims.

a. **Numerosity**. Plaintiff is a representative of the Class, consisting of several hundred members, far too many to join in a single action;

b. **Ascertainability**. Members of the Class are readily identifiable from information in Defendant's possession, custody, and control;

c. **Typicality**. Plaintiff's claims are typical of class claims as each arises from the same Data Breach, the same alleged violations by Defendant, and the same unreasonable manner of notifying individuals about the Data Breach.

d. **Adequacy**. Plaintiff will fairly and adequately protect the proposed Class's interests. His interests do not conflict with the Class's interests, and he has retained counsel experienced in complex class action litigation and data privacy to prosecute this action on the Class's behalf, including as lead counsel.

e. **Commonality**. Plaintiff's and the Class's claims raise predominantly common fact and legal questions that a class wide proceeding can answer for the Class. Indeed, it will be necessary to answer the following questions:

i. Whether Defendant had a duty to use reasonable care in safeguarding Plaintiff's and the Class's PII;

ii. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

iii. Whether Defendant were negligent in maintaining, protecting, and securing PII;

iv. Whether Defendant breached contract promises to safeguard Plaintiff's and the Class's PII;

v. Whether Defendant took reasonable measures to determine the extent of the Data Breach after discovering it;

vi. Whether Defendant's Breach Notice was reasonable;

vii. Whether the Data Breach caused Plaintiff's and the Class's injuries;

viii. What the proper damages measure is; and

ix. Whether Plaintiff and the Class are entitled to damages, treble damages, or injunctive relief.

92. Further, common questions of law and fact predominate over any individualized questions, and a class action is superior to individual litigation or any other available method to fairly and efficiently adjudicate the controversy. The damages available to individual plaintiffs are insufficient to make individual lawsuits economically feasible.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

93. Plaintiff realleges all previous paragraphs as if fully set forth below.

94. Plaintiff and members of the Class entrusted their PII to Defendant. Defendant owed to Plaintiff and the Class a duty to exercise reasonable care in handling and using the PII in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

95. Defendant owed a duty of care to Plaintiff and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PII in accordance with

state-of-the-art industry standards concerning data security would result in the compromise of that PII —just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiff's and the Class's PII by disclosing and providing access to this information to unauthorized third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

96. Defendant owed to Plaintiff and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendant also owed a duty to timely and accurately disclose to Plaintiff and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiff and the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

97. Defendant owed these duties to Plaintiff and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendant knew or should have known would suffer injury-in-fact from Defendant's inadequate security protocols. Defendant actively sought and obtained Plaintiff's and the Class's PII.

98. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendant holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendant's databases containing the PII —whether by malware or otherwise.

99. PII is highly valuable, and Defendant knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiff and the Class and the importance of exercising reasonable care in handling it.

100. Defendant breached its duties by failing to exercise reasonable care in supervising its employees, agents, contractors, vendors, and suppliers, and in handling and securing the PII of Plaintiff and the Class which actually and proximately caused the Data Breach and Plaintiff's and the Class's injury. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiff and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiff's and members of the Class's injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiff and the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

101. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiff and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

102. Plaintiff realleges all previous paragraphs as if fully set forth below.

103. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and the Class's PII.

104. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiff's and the members of the Class's PII.

105. Defendant breached its duties to Plaintiff and Class Members under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII.

106. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential PII.

107. Defendant violated its duty under Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiff's and the Class's PII and not complying with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII Defendant collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to individuals in the event of a breach, which ultimately came to pass.

108. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

109. But for Defendant's wrongful and negligent breach of the duties owed to Plaintiff and members of the Class, Plaintiff and members of the Class would not have been injured.

110. The injury and harm suffered by Plaintiff and members of the Class were the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiff and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

111. Had Plaintiff and the Class known that Defendant did not adequately protect their PII, Plaintiff and members of the Class would not have entrusted Defendant with their PII.

112. Defendant's various violations and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

113. As a direct and proximate result of Defendant's negligence *per se*, Plaintiff and the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen PII, entitling them to damages in an amount to be proven at trial.

114. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiff and Class members have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect their PII in its continued possession.

COUNT III
Breach of an Implied Contract
(On Behalf of Plaintiff and the Class)

115. Plaintiff realleges all previous paragraphs as if fully set forth below.

116. Plaintiff and the Class delivered their PII to Defendant as part of the process of obtaining employment provided by Defendant.

117. Plaintiff and Class Members entered into implied contracts with Defendant under which Defendant agreed to safeguard and protect such information and to timely and accurately notify Plaintiff and Class Members if and when their data had been breached and compromised. Each such contractual relationship imposed on Defendant an implied covenant of good faith and fair dealing by which Defendant was required to perform its obligations and manage Plaintiff's and Class Members' data in a manner which comported with the reasonable expectations of privacy and protection attendant to entrusting such data to Defendant.

118. In providing their PII, Plaintiff and Class Members entered into an implied contract with Defendant whereby Defendant, in receiving such data, became obligated to reasonably safeguard Plaintiff's and the other Class Members' PII.

119. In delivering their PII to Defendant, Plaintiff and Class Members intended and understood that Defendant would adequately safeguard that data.

120. Plaintiff and the Class Members would not have entrusted their PII to Defendant in the absence of such an implied contract.

121. Defendant accepted possession of Plaintiff's and Class Members' PII.

122. Had Defendant disclosed to Plaintiff and Class Members that Defendant did not have adequate computer systems and security practices to secure employees' PII, Plaintiff and members of the Class would not have provided their PII to Defendant.

123. Defendant recognized that employees' PII is highly sensitive and must be protected, and that this protection was of material importance as part of the bargain to Plaintiff and Class Members.

124. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendant.

125. Defendant breached the implied contract with Plaintiff and Class Members by failing to take reasonable measures to safeguard its data.

126. Defendant breached the implied contract with Plaintiff and Class Members by failing to promptly notify them of the access to and exfiltration of their PII.

127. As a direct and proximate result of the breach of contractual duties, Plaintiff and Class Members have suffered actual, concrete, and imminent injuries. The injuries suffered by Plaintiff and the Class Members include: (a) the invasion of privacy; (b) the compromise, disclosure, theft, and unauthorized use of their PII; (c) economic costs associated with the time spent to detect and prevent identity theft, including loss of productivity; (d) monetary costs associated with the detection and prevention of identity theft; (e) economic costs, including time and money, related to incidents of actual identity theft; (f) the emotional distress, fear, anxiety, nuisance and annoyance of dealing related to the theft and compromise

of their PII; (g) the diminution in the value of the services bargained for as Plaintiff and Class Members were deprived of the data protection and security that Defendant promised when Plaintiff and the proposed class entrusted Defendant with their PII; and (h) the continued and substantial risk to Plaintiff and Class Members' PII, which remains in the Defendant's possession with inadequate measures to protect Plaintiff's and Class Members' PII.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

128. Plaintiff realleges all previous paragraphs as if fully set forth below.

129. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

130. Plaintiff and members of the Class conferred a benefit upon Defendant in providing PII to Defendant.

131. Defendant appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendant also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate the employment, services, and goods it sold to Plaintiff and the Class.

132. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiff's and the Class's PII because Defendant failed to adequately protect their PII. Plaintiff and the proposed Class would not have provided their PII to Defendant had they known Defendant would not adequately protect their PII.

133. Defendant should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Invasion of Privacy
Cal. Const. ART. 1 § 1
(On Behalf of Plaintiff and the Class)

134. Plaintiff realleges all previous paragraphs as if fully set forth below.

135. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

136. Defendant owed a duty to Plaintiff and Class Member to keep their PII confidential.

137. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff's and Class Members' PII is highly offensive to a reasonable person.

138. Defendant's reckless and negligent failure to protect Plaintiff's and Class Members' PII constitutes an intentional interference with Plaintiff's and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

139. Defendant's failure to protect Plaintiff's and Class Members' PII acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

140. Defendant knowingly did not notify Plaintiff's and Class Members in a timely fashion about the Data Breach.

141. Because Defendant failed to properly safeguard Plaintiff's and Class Members' PII, Defendant had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

142. As a proximate result of Defendant's acts and omissions, the PII of Plaintiff and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

143. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

144. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their PII. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiff and the Class.

145. Plaintiff and Class Members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiff's and Class Members' PII.

146. Plaintiff and Class Members, seeks compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VI
Violation of California's Unfair Competition Law ("UCL")
Unlawful Business Practice
(Cal Bus. & Prof. Code § 17200, *et seq.*)
(On Behalf of Plaintiff and the Class)

147. Plaintiff realleges all previous paragraphs as if fully set forth below.

148. Defendant engaged in unlawful and unfair business practices in violation of Cal. Bus. & Prof. Code § 17200, et seq. which prohibits unlawful, unfair, or fraudulent business acts or practices ("UCL").

149. Defendant stored the PII of Plaintiff and the Class in its computer systems and knew or should have known it did not employ reasonable, industry standard, and appropriate

security measures that complied with applicable regulations and that would have kept Plaintiff's and the Class's PII secure so as to prevent the loss or misuse of that PII.

150. Defendant failed to disclose to Plaintiff and the Class that their PII was not secure. However, Plaintiff and the Class were entitled to assume, and did assume, that Defendant had secured their PII. At no time were Plaintiff and the Class on notice that their PII was not secure, which Defendant had a duty to disclose.

151. Defendant also violated California Civil Code § 1798.150 by failing to implement and maintain reasonable security procedures and practices, resulting in an unauthorized access and exfiltration, theft, or disclosure of Plaintiff's and the Class's nonencrypted and nonredacted PII.

152. Had Defendant complied with these requirements, Plaintiff and the Class would not have suffered the damages related to the data breach.

153. Defendant's acts, omissions, and misrepresentations as alleged herein were unlawful and in violation of, inter alia, Section 5(a) of the Federal Trade Commission Act.

154. Defendant's conduct was also unfair, in that it violated a clear legislative policy in favor of protecting consumers from data breaches.

155. Defendant's conduct is an unfair business practice under the UCL because it was immoral, unethical, oppressive, and unscrupulous and caused substantial harm. This conduct includes employing unreasonable and inadequate data security despite its business model of actively collecting PII.

156. Defendant also engaged in unfair business practices under the "tethering test." Its actions and omissions, as described above, violated fundamental public policies expressed by the California Legislature. See, e.g., Cal. Civ. Code § 1798.1 ("The Legislature declares

that . . . all individuals have a right of privacy in information pertaining to them . . . The increasing use of computers . . . has greatly magnified the potential risk to individual privacy that can occur from the maintenance of personal information."); Cal. Civ. Code § 1798.81.5(a) ("It is the intent of the Legislature to ensure that personal information about California residents is protected."); Cal. Bus. & Prof. Code § 22578 ("It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern."). Defendant's acts and omissions thus amount to a violation of the law.

157. Instead, Defendant made the PII of Plaintiff and the Class accessible to scammers, identity thieves, and other malicious actors, subjecting Plaintiff and the Class to an impending risk of identity theft. Additionally, Defendant's conduct was unfair under the UCL because it violated the policies underlying the laws set out in the prior paragraph.

158. As a result of those unlawful and unfair business practices, Plaintiff and the Class suffered an injury-in-fact and have lost money or property.

159. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to consumers or competition under all of the circumstances.

160. There were reasonably available alternatives to further Defendant's legitimate business interests, other than the misconduct alleged in this complaint.

161. Therefore, Plaintiff and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant's unlawful and unfair business activities; and any other equitable relief the Court deems proper.

PRAYER FOR RELIEF

Plaintiff and the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiff and the proposed Class, appointing Plaintiff as class representative, and appointing his counsel to represent the Class;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiff and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiff and the Class;

D. Enjoining Defendant from further deceptive practices and making untrue statements Plaintiff the Data Breach and the stolen PII;

E. Awarding Plaintiff and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiff and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiff and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

Dated: September 26, 2024

By: */s/ Andrew G. Gunem*

Andrew G. Gunem (SBN 354042)
Samuel J. Strauss (*Pro Hac Vice* forthcoming)
Raina Borrelli (*Pro Hac Vice* forthcoming)
STRAUSS BORRELLI PLLC
One Magnificent Mile
980 N Michigan Avenue, Suite 1610
Chicago IL, 60611
Telephone: (872) 263-1110
agunem@straussborrelli.com
sam@straussborrelli.com
raina@straussborrelli.com

Attorneys for Plaintiff and Proposed Class

— EXHIBIT A —

P.O. Box 989728
West Sacramento, CA 95798-9728

Raj Kumar Singh Parihar
[redacted]

Enrollment Code [redacted]

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://app.idx.us/account-creation/protect

September 18, 2024

Notice of Data Breach

Dear Raj Kumar Singh Parihar:

MIPS Holding, Inc. ("MIPS") is writing to inform you of an event that may have impacted some of your information. Although there is currently no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On June 26, 2024, we became aware of suspicious activity occurring within our network. We immediately began an investigation, with the assistance of third-party cybersecurity specialists, to determine the scope of the event, contain the event, and ensure our systems were safe. The investigation determined that there was unauthorized access to our network and that certain files and folders were viewed and/or acquired by an unknown actor on June 26, 2024. We then conducted a review to determine what information was impacted and to whom that information related. Based on the review, we determined that your information may have been present in the impacted files and folders.

What Information Was Involved? The investigation determined that your name and Social Security number may have been present in the impacted files and folders.

What We Are Doing. The privacy and security of information in our possession is one of our highest priorities. Upon learning of this event, we took steps to ensure the security of our systems, investigate the event, and report the event to federal law enforcement. Additionally, we are notifying state regulators as required. As part of our commitment to the privacy of information in our care, we continue to implement technical security measures to strengthen the security of our systems. As an additional precaution, we are offering you access to twelve months of complimentary credit monitoring and identity restoration services through IDX, A ZeroFox Company. Information about how to enroll is these services can be found in the attached *Steps You Can Take to Help Protect Personal Information.*

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. We also encourage you to review the attached *Steps You Can Take To Help Protect Personal Information* and to enroll in the credit monitoring and identity protection services we are offering. We will cover the cost of these services; however, you will need to complete the enrollment process.

For More Information. If you have additional questions, please call our dedicated assistance line toll-free at 1-800-939-4170, Monday through Friday, 6:00 AM – 6:00 PM Pacific Time (*except U.S. holidays*). You may also write to MIPS at Attn: Office Manager 2870 Zanker Road, Suite 210, San Jose, CA 94134.

Sincerely,

MIPS Holding, Inc.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 1-202-442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave NW, Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

001229

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

We are offering you access to twelve months of complimentary credit monitoring and identity restoration services through IDX, A ZeroFox Company. IDX identity protection services include: twelve months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. The deadline to enroll is December 18, 2024.

1. **Website and Enrollment.** Scan the QR image or go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. **Activate the credit monitoring** provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. **Telephone.** Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

CM-010

ATTORNEY OR PARTY WITHOUT ATTORNEY *(Name, State Bar number, and address)*:
Andrew G. Gunem (SBN 354042), STRAUSS BORRELLI PLLC, 980 N. Michigan Avenue, Suite 1610, Chicago, IL 60611

TELEPHONE NO.: (872) 263-1100 FAX NO.: (872) 263-1109
EMAIL ADDRESS: agunem@straussborrelli.com
ATTORNEY FOR *(Name)*: RAJ KUMAR SINGH PARIHAR, on behalf of himself and all others similarly situated

FOR COURT USE ONLY

Electronically Filed by Superior Court of CA, County of Santa Clara, on 9/26/2024 5:12 PM Reviewed By: C. Roman Case #24CV448267 Envelope: 16763516

SUPERIOR COURT OF CALIFORNIA, COUNTY OF SANTA CLARA
STREET ADDRESS: 191 N. First Street
MAILING ADDRESS:
CITY AND ZIP CODE: San Jose, CA 95113
BRANCH NAME: Santa Clara - First Street

CASE NAME:
RAJ KUMAR SINGH PARIHAR v. MIPS HOLDING, INC.

CIVIL CASE COVER SHEET
[X] **Unlimited** (Amount demanded exceeds $35,000)
[ ] **Limited** (Amount demanded is $35,000 or less)

Complex Case Designation
[ ] Counter [ ] Joinder
Filed with first appearance by defendant (Cal. Rules of Court, rule 3.402)

CASE NUMBER: 24CV448267
JUDGE:
DEPT.:

Items 1–6 below must be completed (see instructions on page 2).

1. Check **one** box below for the case type that best describes this case:

Auto Tort
[ ] Auto (22)
[ ] Uninsured motorist (46)

Other PI/PD/WD (Personal Injury/Property Damage/Wrongful Death) Tort
[ ] Asbestos (04)
[ ] Product liability (24)
[ ] Medical malpractice (45)
[ ] Other PI/PD/WD (23)

Non-PI/PD/WD (Other) Tort
[X] Business tort/unfair business practice (07)
[ ] Civil rights (08)
[ ] Defamation (13)
[ ] Fraud (16)
[ ] Intellectual property (19)
[ ] Professional negligence (25)
[ ] Other non-PI/PD/WD tort (35)

Employment
[ ] Wrongful termination (36)
[ ] Other employment (15)

Contract
[ ] Breach of contract/warranty (06)
[ ] Rule 3.740 collections (09)
[ ] Other collections (09)
[ ] Insurance coverage (18)
[ ] Other contract (37)

Real Property
[ ] Eminent domain/Inverse condemnation (14)
[ ] Wrongful eviction (33)
[ ] Other real property (26)

Unlawful Detainer
[ ] Commercial (31)
[ ] Residential (32)
[ ] Drugs (38)

Judicial Review
[ ] Asset forfeiture (05)
[ ] Petition re: arbitration award (11)
[ ] Writ of mandate (02)
[ ] Other judicial review (39)

Provisionally Complex Civil Litigation (Cal. Rules of Court, rules 3.400–3.403)
[ ] Antitrust/Trade regulation (03)
[ ] Construction defect (10)
[ ] Mass tort (40)
[ ] Securities litigation (28)
[ ] Environmental/Toxic tort (30)
[ ] Insurance coverage claims arising from the above listed provisionally complex case types (41)

Enforcement of Judgment
[ ] Enforcement of judgment (20)

Miscellaneous Civil Complaint
[ ] RICO (27)
[ ] Other complaint *(not specified above)* (42)

Miscellaneous Civil Petition
[ ] Partnership and corporate governance (21)
[ ] Other petition *(not specified above)* (43)

2. This case [X] is [ ] is not complex under rule 3.400 of the California Rules of Court. If the case is complex, mark the factors requiring exceptional judicial management:
   a. [ ] Large number of separately represented parties
   b. [X] Extensive motion practice raising difficult or novel issues that will be time-consuming to resolve
   c. [X] Substantial amount of documentary evidence
   d. [X] Large number of witnesses
   e. [ ] Coordination with related actions pending in one or more courts in other counties, states, or countries, or in a federal court
   f. [ ] Substantial postjudgment judicial supervision
3. Remedies sought *(check all that apply)*: a. [X] monetary b. [X] nonmonetary; declaratory or injunctive relief c. [X] punitive
4. Number of causes of action *(specify)*: 7
5. This case [X] is [ ] is not a class action suit.
6. If there are any known related cases, file and serve a notice of related case. *(You may use form CM-015.)*

Date: September 26, 2024
Andrew G. Gunem
(TYPE OR PRINT NAME)

(SIGNATURE OF PARTY OR ATTORNEY FOR PARTY)

NOTICE
- Plaintiff must file this cover sheet with the first paper filed in the action or proceeding (except small claims cases or cases filed under the Probate Code, Family Code, or Welfare and Institutions Code). (Cal. Rules of Court, rule 3.220.) Failure to file may result in sanctions.
- File this cover sheet in addition to any cover sheet required by local court rule.
- If this case is complex under rule 3.400 et seq. of the California Rules of Court, you must serve a copy of this cover sheet on all other parties to the action or proceeding.
- Unless this is a collections case under rule 3.740 or a complex case, this cover sheet will be used for statistical purposes only.

Form Adopted for Mandatory Use
Judicial Council of California
CM-010 [Rev. January 1, 2024]

CIVIL CASE COVER SHEET

Cal. Rules of Court, rules 2.30, 3.220, 3.400–3.403, 3.740;
Cal. Standards of Judicial Administration, std. 3.10
www.courts.ca.gov

INSTRUCTIONS ON HOW TO COMPLETE THE COVER SHEET

CM-010

To Plaintiffs and Others Filing First Papers. If you are filing a first paper (for example, a complaint) in a civil case, you **must** complete and file, along with your first paper, the Civil Case Cover Sheet contained on page 1. This information will be used to compile statistics about the types and numbers of cases filed. You must complete items 1 through 6 on the sheet. In item 1, you must check **one** box for the case type that best describes the case. If the case fits both a general and a more specific type of case listed in item 1, check the more specific one. If the case has multiple causes of action, check the box that best indicates the **primary** cause of action. To assist you in completing the sheet, examples of the cases that belong under each case type in item 1 are provided below. A cover sheet must be filed only with your initial paper. Failure to file a cover sheet with the first paper filed in a civil case may subject a party, its counsel, or both to sanctions under rules 2.30 and 3.220 of the California Rules of Court.

To Parties in Rule 3.740 Collections Cases. A "collections case" under rule 3.740 is defined as an action for recovery of money owed in a sum stated to be certain that is not more than $25,000, exclusive of interest and attorney's fees, arising from a transaction in which property, services, or money was acquired on credit. A collections case does not include an action seeking the following: (1) tort damages, (2) punitive damages, (3) recovery of real property, (4) recovery of personal property, or (5) a prejudgment writ of attachment. The identification of a case as a rule 3.740 collections case on this form means that it will be exempt from the general time-for-service requirements and case management rules, unless a defendant files a responsive pleading. A rule 3.740 collections case will be subject to the requirements for service and obtaining a judgment in rule 3.740.

To Parties in Complex Cases. In complex cases only, parties must also use the Civil Case Cover Sheet to designate whether the case is complex. If a plaintiff believes the case is complex under rule 3.400 of the California Rules of Court, this must be indicated by completing the appropriate boxes in items 1 and 2. If a plaintiff designates a case as complex, the cover sheet must be served with the complaint on all parties to the action. A defendant may file and serve no later than the time of its first appearance a joinder in the plaintiff's designation, a counter-designation that the case is not complex, or, if the plaintiff has made no designation, a designation that the case is complex.

CASE TYPES AND EXAMPLES

Auto Tort
- Auto (22)–Personal Injury/Property Damage/Wrongful Death
- Uninsured Motorist (46) *(if the case involves an uninsured motorist claim subject to arbitration, check this item instead of Auto)*

Other PI/PD/WD (Personal Injury/ Property Damage/Wrongful Death) Tort
- Asbestos (04)
  - Asbestos Property Damage
  - Asbestos Personal Injury/ Wrongful Death
- Product Liability *(not asbestos or toxic/environmental)* (24)
- Medical Malpractice (45)
  - Medical Malpractice–Physicians & Surgeons
- Other Professional Health Care Malpractice
- Other PI/PD/WD (23)
  - Premises Liability (e.g., slip and fall)
  - Intentional Bodily Injury/PD/WD (e.g., assault, vandalism)
  - Intentional Infliction of Emotional Distress
  - Negligent Infliction of Emotional Distress
  - Other PI/PD/WD

Non-PI/PD/WD (Other) Tort
- Business Tort/Unfair Business Practice (07)
- Civil Rights (e.g., discrimination, false arrest) *(not civil harassment)* (08)
- Defamation (e.g., slander, libel) (13)
- Fraud (16)
- Intellectual Property (19)
- Professional Negligence (25)
  - Legal Malpractice
  - Other Professional Malpractice *(not medical or legal)*
- Other Non-PI/PD/WD Tort (35)

Employment
- Wrongful Termination (36)
- Other Employment (15)

Contract
- Breach of Contract/Warranty (06)
  - Breach of Rental/Lease Contract *(not unlawful detainer or wrongful eviction)*
  - Contract/Warranty Breach–Seller Plaintiff *(not fraud or negligence)*
  - Negligent Breach of Contract/ Warranty
  - Other Breach of Contract/Warranty
- Collections (e.g., money owed, open book accounts) (09)
  - Collection Case–Seller Plaintiff
  - Other Promissory Note/Collections Case
- Insurance Coverage *(not provisionally complex)* (18)
  - Auto Subrogation
  - Other Coverage
- Other Contract (37)
  - Contractual Fraud
  - Other Contract Dispute

Real Property
- Eminent Domain/Inverse Condemnation (14)
- Wrongful Eviction (33)
- Other Real Property (e.g., quiet title) (26)
  - Writ of Possession of Real Property
  - Mortgage Foreclosure
  - Quiet Title
  - Other Real Property *(not eminent domain, landlord/tenant, or foreclosure)*

Unlawful Detainer
- Commercial (31)
- Residential (32)
- Drugs (38) *(if the case involves illegal drugs, check this item; otherwise, report as Commercial or Residential)*

Judicial Review
- Asset Forfeiture (05)
- Petition Re: Arbitration Award (11)
- Writ of Mandate (02)
  - Writ–Administrative Mandamus
  - Writ–Mandamus on Limited Court Case Matter
  - Writ–Other Limited Court Case Review
- Other Judicial Review (39)
  - Review of Health Officer Order
  - Notice of Appeal–Labor Commissioner Appeals

Provisionally Complex Civil Litigation (Cal. Rules of Court Rules 3.400–3.403)
- Antitrust/Trade Regulation (03)
- Construction Defect (10)
- Claims Involving Mass Tort (40)
- Securities Litigation (28)
- Environmental/Toxic Tort (30)
- Insurance Coverage Claims *(arising from provisionally complex case type listed above)* (41)

Enforcement of Judgment
- Enforcement of Judgment (20)
  - Abstract of Judgment (Out of County)
  - Confession of Judgment *(non-domestic relations)*
  - Sister State Judgment
  - Administrative Agency Award *(not unpaid taxes)*
  - Petition/Certification of Entry of Judgment on Unpaid Taxes
  - Other Enforcement of Judgment Case

Miscellaneous Civil Complaint
- RICO (27)
- Other Complaint *(not specified above)* (42)
  - Declaratory Relief Only
  - Injunctive Relief Only *(non-harassment)*
  - Mechanics Lien
  - Other Commercial Complaint Case *(non-tort/non-complex)*
  - Other Civil Complaint *(non-tort/non-complex)*

Miscellaneous Civil Petition
- Partnership and Corporate Governance (21)
- Other Petition *(not specified above)* (43)
  - Civil Harassment
  - Workplace Violence
  - Elder/Dependent Adult Abuse
  - Election Contest
  - Petition for Name Change
  - Petition for Relief From Late Claim
  - Other Civil Petition

ATTACHMENT CV-5012 T. Phan

CIVIL LAWSUIT NOTICE

Superior Court of California, County of Santa Clara
191 North First St., San José, CA 95113

CASE NUMBER: 24CV448267

PLEASE READ THIS ENTIRE FORM

PLAINTIFF (the person suing): Within 60 days after filing the lawsuit, you must serve each Defendant with the *Complaint*, *Summons*, an *Alternative Dispute Resolution (ADR) Information Sheet*, and a copy of this *Civil Lawsuit Notice*, and you must file written proof of such service.

DEFENDANT (The person sued): **You must do each of the following to protect your rights:**

1. You must file a **written response** to the *Complaint, using the proper legal form or format,* in the Clerk's Office of the Court, within **30 days** of the date you were served with the *Summons* and *Complaint*;
2. You must serve by mail a copy of your written response on the Plaintiff's attorney or on the Plaintiff if Plaintiff has no attorney (to "serve by mail" means to have an adult other than yourself mail a copy); and
3. You must attend the first Case Management Conference.

Warning: If you, as the Defendant, do not follow these instructions, you may automatically lose this case.

RULES AND FORMS: You must follow the California Rules of Court and the Superior Court of California, County of Santa Clara Local Civil Rules and use proper forms. You can obtain legal information, view the rules and receive forms, free of charge, from the Self-Help Center at 201 North First Street, San José or at https://www.scscourt.org/self_help/civil/civil_help.shtml.

- State Rules and Judicial Council Forms: https://www.courts.ca.gov/formsrules.htm
- Local Rules and Forms: https://www.scscourt.org/forms_filing.shtml and https://www.scscourt.org/court_divisions/civil/civil_rules/civil_rules.shtml

CASE MANAGEMENT CONFERENCE (CMC): You must meet with the other parties and discuss the case, in person or by telephone at least 30 calendar days before the CMC. You must also fill out, file and serve a *Case Management Statement* (Judicial Council form CM-110) at least 15 calendar days before the CMC.

You or your attorney must appear at the CMC. *You may have the option, or be required, to appear remotely – see Local Civil Rule 8.*

Your Case Management Judge is: Zayner, Theodore C **Department:** 19

The 1st CMC is scheduled for: (Completed by Clerk of Court)

Date: 03/05/2025 **Time:** 2:30pm in **Department:** 19

The next CMC is scheduled for: (Completed by party if the 1st CMC was continued or has passed)

Date: _____ **Time:** _____ in **Department:** _____

ALTERNATIVE DISPUTE RESOLUTION (ADR): If all parties have appeared and filed a completed *ADR Stipulation Form* (local form CV-5008) at least 30 days before the CMC, the Court will cancel the CMC and mail notice of an ADR Status Conference. Visit the Court's website at https://www.scscourt.org/court_divisions/civil/adr/civil_adr.shtml or call the ADR Administrator (408-828-8547) for more information.

WARNING: Sanctions may be imposed if you do not follow the California Rules of Court or the Local Rules of Court.

SUM-100

SUMMONS
(CITACION JUDICIAL)

FOR COURT USE ONLY
(SOLO PARA USO DE LA CORTE)

E-FILED
9/26/2024 5:12 PM
Clerk of Court
Superior Court of CA,
County of Santa Clara
24CV448267
Reviewed By: C. Roman
Envelope: 16763516

NOTICE TO DEFENDANT:
(AVISO AL DEMANDADO):
MIPS HOLDING, INC.

YOU ARE BEING SUED BY PLAINTIFF:
(LO ESTÁ DEMANDANDO EL DEMANDANTE):
RAJ KUMAR SINGH PARIHAR, on behalf of himself and all others similarly situated

NOTICE! You have been sued. The court may decide against you without your being heard unless you respond within 30 days. Read the information below.

You have 30 CALENDAR DAYS after this summons and legal papers are served on you to file a written response at this court and have a copy served on the plaintiff. A letter or phone call will not protect you. Your written response must be in proper legal form if you want the court to hear your case. There may be a court form that you can use for your response. You can find these court forms and more information at the California Courts Online Self-Help Center (*www.courtinfo.ca.gov/selfhelp*), your county law library, or the courthouse nearest you. If you cannot pay the filing fee, ask the court clerk for a fee waiver form. If you do not file your response on time, you may lose the case by default, and your wages, money, and property may be taken without further warning from the court.

There are other legal requirements. You may want to call an attorney right away. If you do not know an attorney, you may want to call an attorney referral service. If you cannot afford an attorney, you may be eligible for free legal services from a nonprofit legal services program. You can locate these nonprofit groups at the California Legal Services Web site (*www.lawhelpcalifornia.org*), the California Courts Online Self-Help Center (*www.courtinfo.ca.gov/selfhelp*), or by contacting your local court or county bar association. **NOTE:** The court has a statutory lien for waived fees and costs on any settlement or arbitration award of $10,000 or more in a civil case. The court's lien must be paid before the court will dismiss the case.
¡AVISO! *Lo han demandado. Si no responde dentro de 30 días, la corte puede decidir en su contra sin escuchar su versión. Lea la información a continuación.*

Tiene 30 DÍAS DE CALENDARIO después de que le entreguen esta citación y papeles legales para presentar una respuesta por escrito en esta corte y hacer que se entregue una copia al demandante. Una carta o una llamada telefónica no lo protegen. Su respuesta por escrito tiene que estar en formato legal correcto si desea que procesen su caso en la corte. Es posible que haya un formulario que usted pueda usar para su respuesta. Puede encontrar estos formularios de la corte y más información en el Centro de Ayuda de las Cortes de California (www.sucorte.ca.gov), en la biblioteca de leyes de su condado o en la corte que le quede más cerca. Si no puede pagar la cuota de presentación, pida al secretario de la corte que le dé un formulario de exención de pago de cuotas. Si no presenta su respuesta a tiempo, puede perder el caso por incumplimiento y la corte le podrá quitar su sueldo, dinero y bienes sin más advertencia.

Hay otros requisitos legales. Es recomendable que llame a un abogado inmediatamente. Si no conoce a un abogado, puede llamar a un servicio de remisión a abogados. Si no puede pagar a un abogado, es posible que cumpla con los requisitos para obtener servicios legales gratuitos de un programa de servicios legales sin fines de lucro. Puede encontrar estos grupos sin fines de lucro en el sitio web de California Legal Services, (www.lawhelpcalifornia.org), en el Centro de Ayuda de las Cortes de California, (www.sucorte.ca.gov) o poniéndose en contacto con la corte o el colegio de abogados locales. AVISO: Por ley, la corte tiene derecho a reclamar las cuotas y los costos exentos por imponer un gravamen sobre cualquier recuperación de $10,000 ó más de valor recibida mediante un acuerdo o una concesión de arbitraje en un caso de derecho civil. Tiene que pagar el gravamen de la corte antes de que la corte pueda desechar el caso.

The name and address of the court is:
(El nombre y dirección de la corte es): Superior Court of California, Santa Clara

Santa Clara - First Street, 191 N. First Street, San Jose, CA 95113

CASE NUMBER:
(Número del Caso): 24CV448267

The name, address, and telephone number of plaintiff's attorney, or plaintiff without an attorney, is:
(El nombre, la dirección y el número de teléfono del abogado del demandante, o del demandante que no tiene abogado, es):
Andrew G. Gunem, STRAUSS BORRELLI PLLC, 980 N. Michigan Avenue, Suite 1610, Chicago, IL 60611

DATE: September 26, 2024
(Fecha) 9/26/2024 5:12 PM Clerk of Court Clerk, by *(Secretario)* C. Roman , Deputy *(Adjunto)*

(For proof of service of this summons, use Proof of Service of Summons *(form POS-010).)*
(Para prueba de entrega de esta citatión use el formulario Proof of Service of Summons, *(POS-010)).*

[SEAL]

NOTICE TO THE PERSON SERVED: You are served
1. ☐ as an individual defendant.
2. ☐ as the person sued under the fictitious name of *(specify):*
3. ☐ on behalf of *(specify):*
   under: ☐ CCP 416.10 (corporation) ☐ CCP 416.60 (minor)
   ☐ CCP 416.20 (defunct corporation) ☐ CCP 416.70 (conservatee)
   ☐ CCP 416.40 (association or partnership) ☐ CCP 416.90 (authorized person)
   ☐ other *(specify):*
4. ☐ by personal delivery on *(date):*

Form Adopted for Mandatory Use
Judicial Council of California
SUM-100 [Rev. July 1, 2009]

SUMMONS

Code of Civil Procedure §§ 412.20, 465
www.courts.ca.gov