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

[Additional Counsel Appear on Signature Page]

Counsel for Plaintiffs and The Proposed Class

SUPERIOR COURT OF THE STATE OF CALIFORNIA

COUNTY OF LOS ANGELES

MARC-ANTONY HALLIDAY, on behalf of himself and all others similarly situated,

Plaintiff,

v.

PANDA RESTAURANT GROUP, INC.,

Defendant.

CASE NO. 24STCV12667

AMENDED CLASS ACTION COMPLAINT

COMPLAINT FOR:

(1) NEGLIGENCE
(2) BREACH OF IMPLIED CONTRACT
(3) UNJUST ENRICHMENT
(4) VIOLATION OF THE CAL. CONSUMER PRIVACY ACT, CAL. CIV. CODE § 1798.150
(5) VIOLATION OF THE CAL. UNFAIR COMPETITION LAW, CAL. BUS. & PROF. CODE § 17200

DEMAND FOR JURY TRIAL

Marc-Antony Halliday, Victoria Ruggieri, Emily Flessas, Matthew Klepper, Steven Jackson, Elizabeth Little (née Jimenez), Stephanie Sarfo, Silas Davis, and Joshua Oluwalowo (collectively "Plaintiffs"), through their attorneys, individually and on behalf of all others similarly situated, bring this Consolidated Amended Class Action Complaint against Defendant the Panda Restaurant Group, Inc. ("Defendant" or "Panda"). Plaintiffs allege the following on information and belief—except as to their own actions, counsel's investigations, and facts of public record.

SUMMARY OF THE CASE

1. This putative class action arises from Defendant Panda's negligent failure to implement and maintain reasonable cybersecurity procedures and practices with respect to the sensitive and confidential personal information Panda obtains from its employees and/or customers, and the consequent cybersecurity breach of its systems that occurred on around March 7-11, 2024. Panda is restaurant group based in Rosemead, California, and operates approximately 2,300 restaurants in 34 states. In connection with its business, Panda collects, stores, and processes personal information and data for its customers and employees.

2. Due to its lack of adequate cybersecurity measures, Panda suffered a data breach on or around March 7-11, 2024. Panda waited weeks after the data breach to inform impacted parties that their personal identifying information ("PII") was the target of a data breach.

3. Plaintiffs bring this class action complaint to redress these injuries, on behalf of themselves and a class of similarly situated persons. Plaintiffs assert claims on behalf of a class for negligence, breach of implied contract, and unjust enrichment. Plaintiffs also bring claims for violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150 and violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code § 17200 *et seq.* Plaintiffs seek, among other things, compensatory damages, punitive and exemplary damages, injunctive relief,

attorneys' fees, and costs of suit.

PARTIES

4. Plaintiff Marc-Antony Halliday is a citizen and resident of the State of California who resides in Paso Robles, California, and whose personal identification information was part of the data breach at issue in this litigation.

5. Plaintiff Victoria Ruggieri is a citizen and resident of the Commonwealth of Pennsylvania who resides in Harrisburg, Pennsylvania, and whose personal identification information was part of the data breach at issue in this litigation.

6. Plaintiff Emily Flessas is a citizen and resident of the State of Wisconsin who resides in Milwaukee, Wisconsin, and whose personal identification information was part of the data breach at issue in this litigation.

7. Plaintiff Matthew Klepper is a citizen and resident of the State of Tennessee who resides in Kingsport, Tennessee, and whose personal identification information was part of the data breach at issue in this litigation.

8. Plaintiff Steven Jackson is a citizen and resident of the State of Utah who resides in Saratoga Springs, Utah, and whose personal identification information was part of the data breach at issue in this litigation.

9. Plaintiff Elizabeth Little (née Jimenez) is a citizen and resident of the State of Texas who resides in Clyde, Texas, and whose personal identification information was part of the data breach at issue in this litigation.

10. Plaintiff Stephanie Sarfo is a citizen and resident of the State of West Virginia who resides in Martinsburg, West Virginia, and whose personal identification information was part of the data breach at issue in this litigation.

11. Plaintiff Silas Davis is a citizen and resident of the State of Ohio who resides in

Findlay, Ohio, and whose personal identification information was part of the data breach at issue in this litigation.

12. Plaintiff Joshua Oluwalowo is a citizen and resident of the State of Minnesota who resides in Brooklyn Park, Minnesota, and whose personal identification information was part of the data breach at issue in this litigation.

13. Defendant Panda Restaurant Group, Inc. is a California corporation organized and existing under the laws of the State of California with its principal place of business in Rosemead, California.

14. Plaintiffs bring this action on behalf of themselves, 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 of similarly situated persons pursuant to California Code of Civil Procedure § 382.

JURISDICTION & VENUE

15. This Court has general personal jurisdiction over Panda because, at all relevant times, Panda is and has been a California company. Panda is a California corporation and registered to do business in California with the California Secretary of State. Further, it has had systematic and continuous contacts with the State of California. Panda is based in Rosemead, California, and regularly contracts with a multitude of businesses and organizations in California.

16. Furthermore, this Court has specific personal jurisdiction over Panda because the claims in this action stem from its specific contacts with the State of California — namely, Panda's collection, maintenance, and processing of the personal data of Californians in connection with its business, Panda'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 on or around March 7-11, 2024, that resulted from Panda's failures.

17. Venue is proper in the County of Los Angeles in accordance with Code of Civil Procedure § 395.5 because the alleged wrongs occurred in this county and Panda conducts business within Los Angeles County.

FACTUAL BACKGROUND

18. Panda is a restaurant group that operates more than 2,000 restaurants in over 30 states. The company is based in Rosemead, California.

19. In connection with its business, Panda collects, stores, and processes sensitive personal data for hundreds, if not thousands, of customers and current and former employees. In doing so, on information and belief, Panda retains sensitive information related to payroll records such as direct deposit information, bank account information, health information, addresses, and Social Security numbers, among other things.

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

21. Notably, on Defendant's employee-directed website "pandacareers.com," Defendant advertises two privacy policies—wherein Defendant promises its current and former employees that it will protect their PII.

22. First, via its "Panda Restaurant Group, Inc. Privacy Policy," Defendant declares that:

a. "We respect your privacy and are committed to protecting it through our compliance with this policy."[1]

b. "The following statement discloses the privacy practices of Panda Restaurant Group, Inc., and its affiliates, subsidiaries and related entities including, but not limited to Panda Express, Panda Inn, Wasabi, Uncle Tetsu, Yakiya, and Hibachi San locations owned and operated by us (collectively, 'Panda' or 'we' or 'us')."[2]

[1] *Panda Restaurant Group, Inc. Privacy Policy*, PANDA CAREERS (Jan. 4, 2023) https://www.pandacareers.com/prg-privacy-policy.
[2] *Id.*

c. "This policy describes the types of information we may collect from you or that you may provide through various channels such as our websites, mobile apps, visiting our stores and other interactions (collectively 'Services'), and our practices for collecting, using, maintaining, protecting, and disclosing that information."[3]

d. "We collect several types of information from and about users of our Services . . . include[ing] contact information, demographic information and opinions, including information by which you may be personally identified, such as name, postal address, e-mail address, user ID, telephone number, payment information or any other identifier by which you may be contacted online or offline ('personal information')."[4]

e. "In the 'Careers' section of our websites we have an employment application. The completion of this form is voluntary, and all information collected is routed to Human Resources in the form of an e-mail or hiring/recruiting website. Information you submit online through this website may be shared by and among Panda and its subsidiaries and affiliates. ***We protect the confidentiality of such information*** sent to Panda."[5]

f. "We do not make any of the information collected available to third parties other than solely on our behalf."[6]

g. "We will use reasonable efforts to keep your personal information private except as otherwise provided in this Privacy Policy."[7]

h. "***We will not share the personal information with any unaffiliated third parties***, unless such disclosure is necessary to (a) comply with a court order or other legal process, (b) protect your rights or our property; or (c) enforce the Terms and Conditions for Services of this website."[8]

---

[3] *Id*.
[4] *Id*.
[5] *Id*. (emphasis added).
[6] *Id*.
[7] *Id*.
[8] *Id*. (emphasis added).

i. "Panda only uses and discloses Sensitive Personal Information as necessary in connection with the performance of services and the provision of goods, compliance with federal, state, or local laws, and as otherwise permitted by California Privacy Law."[9]

j. "Protecting your personal information is important to us."[10]

k. "We maintain administrative, technical, and physical safeguards designed to help protect against unauthorized use, disclosure, alteration, or destruction of the personal information we collect on our websites."[11]

23. Second, via its "Job Applicant Privacy Notice," Defendant induces job applications by promising the following:

a. "This Job Applicant Privacy Notice discloses the privacy practices of Panda Restaurant Group, Inc., and its affiliates, subsidiaries and related entities including, but not limited to Panda Express . . . with respect to any and all personal information collected in connection with your application for employment and hiring with Panda[.]"[12]

b. "Panda only uses and discloses sensitive personal information as necessary to perform functions related to your application and hiring and to comply with federal, state, or local laws, and otherwise as permitted California Privacy Law."[13]

c. "The security and confidentiality of your Recruitment Information matters to us. That's why we have technical, administrative, and physical controls in place to protect your Recruitment Information from unauthorized access, use, and disclosure."[14]

d. "We do not use or disclose Recruitment Information that is sensitive personal information except as necessary to support and process your application, to

[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *Job Applicant Privacy Policy*, PANDA CAREERS (July 7, 2023) https://www.pandacareers.com/privacy-policy.
[13] *Id.*
[14] *Id.*

comply with law and regulation, and otherwise as permitted by California Privacy Law."[15]

24. Panda knew that it was a prime target for hackers given the significant amount of sensitive personal information in its possession, custody and/or control related to its customers and employees. Panda's knowledge is underscored by the massive number of data breaches that have occurred in recent years.

25. Despite knowing the prevalence of data breaches, Panda failed to prioritize data security by adopting reasonable data security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. Panda has the resources to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized breaches. Panda 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 Plaintiffs' and Class Members' data were protected.

26. Specifically, on or around March 7-11, 2024, Panda experienced a cybersecurity breach (the "Data Breach). Panda waited until the end of April 2024 to disclose this Data Breach to impacted individuals.

27. On information and belief, the personal information Panda collects and which was impacted by the cybersecurity attack includes an individual's name, Social Security number and date of birth.

28. On or around April 30, 2024, Panda mailed written notice of the Data Breach to impacted individuals. Panda confirmed that an unauthorized party was able to gain access to its systems on or around March 7-11, 2024. Plaintiffs received a copy of the Data Breach notice via United States mail service confirming that their PII was part of the Data Breach.

29. Panda's Data Breach notice contained cursory information about the breach, and Panda has continued to provide few, if any, detailed specifics about the breach to the public and/or individuals impacted.

30. Upon information and belief, the individuals responsible for the Data Breach stole

[15] *Id.*

the personal information of all employees of Panda, and the personal identifying information of its customers, including Plaintiffs' personal identifying information. Because of the nature of the breach and of the personal information stored or processed by Panda, Plaintiffs are informed and believe that all categories of personal information were further subject to unauthorized access, disclosure, theft, exfiltration, modification, use, or destruction. Plaintiffs are informed and believe that criminals would have no purpose for hacking Panda 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 Panda.

31. The personal information exposed by Panda 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.

32. 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.

33. 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.

34. 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.

35. 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.

36. 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.

37. According to the FTC, the need for data security should be factored into all business decision-making.[16] 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.[17] 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 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.

38. 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.[18]

39. 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

[16] *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 February 6, 2025).
[17] *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 February 6, 2022).
[18] *See id.*

practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45.

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

41. 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.[19] 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 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.

[19] *How to Protect Your Networks from Ransomware*, FBI, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (last viewed February 6, 2025).

- 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.[20]

42. Panda 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.

43. Panda'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 Panda that collect, process, and store massive amounts of data on cloud-based systems, including but not limited to their Employee and Distributor online portals, as being particularly vulnerable to cyberattacks because of the value of the personal information that they collect and maintain. Accordingly, Panda knew or should have known that it was a prime target for hackers.

44. 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

[20] *Id.*

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.[21]

45. Upon information and belief, Panda did not encrypt Plaintiffs' and Class Members' personal information involved in the Data Breach.

46. Despite knowing the prevalence of data breaches, Panda failed to prioritize cybersecurity by adopting reasonable security measures to prevent and detect unauthorized access to its highly sensitive systems and databases. Panda has the resources to prevent an attack, but neglected to adequately invest in cybersecurity, despite the growing number of well-publicized breaches. Panda failed to fully implement each and all of the above-described data security best practices. Panda 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 Plaintiffs' and Class Members' data were protected.

Plaintiffs Common Experiences

47. Defendant received highly sensitive PII from Plaintiffs in connection with the services Plaintiffs received or requested. As a result, Plaintiffs' information was among the data an unauthorized third party accessed in the Data Breach.

48. Plaintiffs were and are very careful about sharing their PII. Plaintiffs have never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

49. Plaintiffs stored any documents containing their PII in a safe and secure location or destroyed the documents. Moreover, Plaintiffs diligently chose unique usernames and passwords for their various online accounts.

50. Plaintiffs took reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for employment purposes only, and to make only authorized disclosures of this information.

51. The Notice from Defendant (the website version of this Notice, which is substantially similar in content to the Notices received by Representative Plaintiffs and the Class)

[21] 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 February 6, 2025).

notified Plaintiffs that Defendant's network had been accessed and that Plaintiffs' PII may have been involved in the Data Breach.

52. Furthermore, Defendant's Notice directed Plaintiffs to be vigilant and to take certain steps to protect their PII and otherwise mitigate their damages.

53. As a result of the Data Breach, Plaintiffs heeded Defendant's warnings and spent time dealing with the consequences of the Data Breach, which included time spent verifying the legitimacy of the Notice and self-monitoring their accounts and credit reports to ensure no fraudulent activity had occurred. This time has been lost forever and cannot be recaptured.

54. Plaintiffs suffered actual injury in the form of damages to and diminution in the value of Plaintiffs' PII—a form of intangible property that Plaintiffs entrusted to Defendant, which was compromised in and because of the Data Breach.

55. Plaintiffs suffered lost time, annoyance, interference, and inconvenience because of the Data Breach and have anxiety and increased concerns for the loss of privacy, as well as anxiety over the impact of cybercriminals accessing, using, and selling Plaintiffs' PII.

56. Plaintiffs have a continuing interest in ensuring that Plaintiffs' PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

57. As a direct and foreseeable result of Panda's negligent failure to implement and maintain reasonable data security procedures and practices and the resultant breach of its systems, Plaintiffs 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.

58. Upon information and belief, Plaintiffs' 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.

59. 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.[22]

60. Furthermore, Plaintiffs and Class Members are well aware that their sensitive personal information, including Social Security numbers and potentially banking and credit card information, risks being available to other cybercriminals on the dark web. Accordingly, Plaintiffs and Class Members have suffered harm in the form of increased stress, fear, and risk of identity theft and fraud resulting from the data breach. Additionally, Plaintiffs 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.

Plaintiff Halliday's Experience and Injuries

61. Plaintiff Marc-Antony Halliday is a natural person and citizen of California. He lives in Paso Robles, California, where he intends to remain.

62. Plaintiff Halliday was an employee of Defendant. Thus, Defendant obtained and maintained Plaintiff Halliday's PII. And as a result, Plaintiff Halliday was injured by Defendant's Data Breach.

63. Upon information and belief, the PII that Defendant obtained and maintained includes Plaintiff Halliday's name, date of birth, address, Social Security number, driver's license

[22] *Identify Theft and Your Social Security Number*, Social Security Administration, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited February 6, 2025).

number, government ID number, passport number, state ID number, financial information, financial account number, credit card number, debit card number, health insurance information, and/or medical information.

64. As a condition of his employment with Defendant, Plaintiff Halliday provided Defendant with his PII. Defendant used that PII to facilitate its employment of Plaintiff Halliday, including payroll, and required Plaintiff Halliday to provide that PII in order to obtain employment and payment for that employment.

65. Plaintiff Halliday highly values the privacy of his PII. As such, he is careful to make sure that his PII remains private and secure. And Plaintiff Halliday does not knowingly disclose his PII in an unsecure manner over the internet or otherwise. Thus, he would not have disclosed his PII to Defendant if Defendant was forthcoming about its inadequate data security.

66. Plaintiff Halliday provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Halliday's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

67. Plaintiff Halliday reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII.

68. Plaintiff Halliday does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

69. Plaintiff Halliday received a Notice of Data Breach in the mail directly from Defendant. Thus, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

70. Through its Data Breach, Defendant compromised Plaintiff Halliday's PII. And upon information and belief, many types of Plaintiff Halliday's PII were compromised in the Data

Breach—given that Defendant's disclosure to the Texas Attorney General revealed that an extremely broad range of PII was exposed.

71. Plaintiff Halliday has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Halliday to take those steps in its breach notice.

72. Specifically, Plaintiff has spent approximately multiple hours inter alia:

a. researching the Data Breach to determine the extent of his exposure;

b. carefully reviewing his accounts for suspicious activity;

c. changing the passwords on his various accounts; and

d. contacting his bank and putting fraud detection measures in place.

73. And in the aftermath of the Data Breach, Plaintiff Halliday has suffered from a spike in spam and scam including:

a. scam emails purportedly about investments and cryptocurrencies (these began right after the Data Breach);

b. scam phone calls; and

c. scam texts purportedly related to medical appointments and a letter purportedly from a medical facility (which Plaintiff does not recognize).

74. Plaintiff Halliday fears for his personal financial security and worries about what information was exposed in the Data Breach. And because of Defendant's Data Breach, Plaintiff Halliday has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Halliday's injuries are precisely the type of injuries that the law contemplates and addresses.

75. Plaintiff Halliday suffered actual injury from the exposure and theft of his PII—

which violates his rights to privacy.

76. Plaintiff Halliday suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

77. Plaintiff Halliday suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Halliday's PII right in the hands of criminals.

78. Because of the Data Breach, Plaintiff Halliday anticipates spending considerable amounts of time and money to try and mitigate his injuries.

79. Today, Plaintiff Halliday has a continuing interest in ensuring that his PII—which, upon information and belief, remains insecurely backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Ruggeri's Experiences and Injuries

80. Plaintiff Victoria Ruggeri is a natural person and citizen of Pennsylvania. She lives in Harrisburg, Pennsylvania, where she intends to remain.

81. Plaintiff Ruggeri is a former employee of Defendant—having worked for Defendant in or around 2022. Thus, Defendant obtained and maintained Plaintiff Ruggeri's PII. And as a result, Plaintiff Ruggeri was injured by Defendant's Data Breach.

82. Upon information and belief, the PII that Defendant obtained and maintained includes Plaintiff Ruggeri's name, date of birth, address, Social Security number, driver's license number, government ID number, passport number, state ID number, financial information, financial account number, credit card number, debit card number, health insurance information, and/or medical information.[23]

[23] *See Data Security Breach Reports*, ATTY GEN TEXAS (May 3, 2024)

83. As a condition of her employment with Defendant, Plaintiff Ruggeri provided Defendant with her PII. Defendant used that PII to facilitate its employment of Plaintiff Ruggeri, including payroll, and required Plaintiff Ruggeri to provide that PII in order to obtain employment and payment for that employment.

84. Plaintiff Ruggeri highly values the privacy of her PII. As such, she is careful to make sure that her PII remains private and secure. And Plaintiff Ruggeri does not knowingly disclose her PII in an unsecure manner over the internet or otherwise. Thus, she would not have disclosed her PII to Defendant if Defendant was forthcoming about its inadequate data security.

85. Plaintiff Ruggeri provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Ruggeri's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

86. Plaintiff Ruggeri reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII.

87. Plaintiff Ruggeri does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

88. Plaintiff Ruggeri received a Notice of Data Breach in the mail directly from Defendant. Thus, on information and belief, Plaintiff Ruggeri's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

89. Through its Data Breach, Defendant compromised Plaintiff Ruggeri's name, date of birth, and Social Security number. However, upon information and belief, other types of Plaintiff Ruggeri's PII were compromised in the Data Breach—given that Defendant's disclosure to the Texas Attorney General revealed that an extremely broad range of PII was exposed.

---

https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (listing the types of information affected by Panda's Data Breach).

90. Plaintiff Ruggeri has ***already*** suffered from identity theft and fraud:

a. "Mastercard" notified her via letter that an application in her name was approved (but Plaintiff Ruggeri never submitted any such application).

b. Her "Chime" checking account—which is Plaintiff Ruggeri's primary checking account—was subjected to fraudulent charges of $15.00 and $10.00 in or around May 10, 2024. Thereafter, Chime closed her checking account (which interfered with her ability to access her funds). Later, Plaintiff Ruggeri appealed the closing of her account, and her account was eventually reinstated—but she was forced to wait to receive a new card.

c. "CashApp" closed her account in the fallout of the Data Breach; and

d. "TurboTax" notified her that her federal tax return was being completed (but Plaintiff was not responsible for this activity). Worryingly, the identity thief was using TurboTax's "RaceMode" feature and had successfully "complete[d]" inputting all of Plaintiff's "[p]ersonal info."

91. And in the aftermath of the Data Breach, Plaintiff Ruggeri has suffered from a spike in spam and scam phone calls.

92. Additionally, Plaintiff Ruggeri appears to have been targeted by a flood of phishing emails—for example, in one day, she received at least six (6) back-to-back emails purportedly from "Paypal" declaring that:

a. "You changed your password[;]"

b. "Hello, Victoria Ruggeri[;]" and

c. "Victoria Ruggeri, we're confirming what changed."

93. Plaintiff Ruggeri has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed

Plaintiff Ruggeri to take those steps in its breach notice.

94. Specifically, Plaintiff Ruggeri spent approximately 10–20 hours attempting to mitigate the fallout of the Data Breach by, *inter alia*:

a. researching the Data Breach to determine the extent of her exposure;

b. carefully reviewing her accounts for suspicious activity (including Chime, CashApp, TurboTax, and her email); and

c. contacting Chime and appealing the closure of her account.

95. Plaintiff Ruggeri fears for her personal financial security and worries about what information was exposed in the Data Breach. And because of Defendant's Data Breach, Plaintiff Ruggeri has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Ruggeri's injuries are precisely the type of injuries that the law contemplates and addresses.

96. Plaintiff Ruggeri suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

97. Plaintiff Ruggeri suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

98. Plaintiff Ruggeri suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Ruggeri's PII right in the hands of criminals.

99. Because of the Data Breach, Plaintiff Ruggeri anticipates spending considerable amounts of time and money to try and mitigate her injuries.

100. Today, Plaintiff Ruggeri has a continuing interest in ensuring that her PII—which,

upon information and belief, remains insecurely backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Flessas's Experiences and Injuries

101. Plaintiff Emily Flessas is a natural person and citizen of Wisconsin. She lives in Milwaukee, Wisconsin, where she intends to remain.

102. Plaintiff Flessas is a former employee of Defendant—having worked for Defendant until 2024. Thus, Defendant obtained and maintained Plaintiff Flessas's PII. And as a result, Plaintiff Flessas was injured by Defendant's Data Breach.

103. Upon information and belief, the PII that Defendant obtained and maintained includes Plaintiff Flessas's name, date of birth, address, Social Security number, driver's license number, government ID number, passport number, state ID number, financial information, financial account number, credit card number, debit card number, health insurance information, and/or medical information.[24]

104. As a condition of her employment with Defendant, Plaintiff Flessas provided Defendant with her PII. Defendant used that PII to facilitate its employment of Plaintiff Flessas, including payroll, and required Plaintiff Flessas to provide that PII in order to obtain employment and payment for that employment.

105. Plaintiff Flessas highly values the privacy of her PII. As such, she is careful to make sure that her PII remains private and secure. And Plaintiff Flessas does not knowingly disclose her PII in an unsecure manner over the internet or otherwise. Thus, she would not have disclosed her PII to Defendant if Defendant was forthcoming about its inadequate data security.

106. Plaintiff Flessas provided her PII to Defendant and trusted the company would use

[24] *See Data Security Breach Reports*, ATTY GEN TEXAS (May 3, 2024) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (listing the types of information affected by Panda's Data Breach).

reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Flessas's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

107. Plaintiff Flessas reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII.

108. Plaintiff Flessas does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

109. Plaintiff Flessas received a Notice of Data Breach in the mail directly from Defendant. Thus, on information and belief, Plaintiff Flessas's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

110. Through its Data Breach, Defendant compromised Plaintiff Flessas's PII. And upon information and belief, many types of Plaintiff Flessas's PII were compromised in the Data Breach—given that Defendant's disclosure to the Texas Attorney General revealed that an extremely broad range of PII was exposed.

111. Plaintiff Flessas has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff Flessas to take those steps in its breach notice.

112. Specifically, Plaintiff Flessas has spent approximately 2–3 hours, *inter alia*:

a. researching the Data Breach to determine the extent of her exposure; and

b. carefully reviewing her financial accounts for suspicious activity.

113. And in the aftermath of the Data Breach, Plaintiff Flessas has suffered from a spike in spam and scam text messages and phone calls.

114. Plaintiff Flessas fears for her personal financial security and worries about what information was exposed in the Data Breach. And because of Defendant's Data Breach, Plaintiff

Flessas has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Flessas's injuries are precisely the type of injuries that the law contemplates and addresses.

115. Plaintiff Flessas suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

116. Plaintiff Flessas suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

117. Plaintiff Flessas suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Flessas's PII right in the hands of criminals.

118. Because of the Data Breach, Plaintiff Flessas anticipates spending considerable amounts of time and money to try and mitigate her injuries.

119. Today, Plaintiff Flessas has a continuing interest in ensuring that her PII—which, upon information and belief, remains insecurely backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Sarfo's Experiences and Injuries

120. Plaintiff Stephanie Sarfo is a natural person and citizen of West Virginia. She lives in Martinsburg, West Virginia, where she intends to remain.

121. Plaintiff Sarfo is a former employee of Defendant—having worked for Defendant from approximately 2022 until 2023. Thus, Defendant obtained and maintained Plaintiff Sarfo's PII. And as a result, Plaintiff Sarfo was injured by Defendant's Data Breach.

122. Upon information and belief, the PII that Defendant obtained and maintained

includes Plaintiff Sarfo's name, date of birth, address, Social Security number, driver's license number, government ID number, passport number, state ID number, financial information, financial account number, credit card number, debit card number, health insurance information, and/or medical information.[25]

123. As a condition of her employment with Defendant, Plaintiff Sarfo provided Defendant with her PII. Defendant used that PII to facilitate its employment of Plaintiff Sarfo, including payroll, and required Plaintiff Sarfo to provide that PII in order to obtain employment and payment for that employment.

124. Plaintiff Sarfo highly values the privacy of her PII. As such, she is careful to make sure that her PII remains private and secure. And Plaintiff Sarfo does not knowingly disclose her PII in an unsecure manner over the internet or otherwise. Thus, she would not have disclosed her PII to Defendant if Defendant was forthcoming about its inadequate data security.

125. Plaintiff Sarfo provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Sarfo's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

126. Plaintiff Sarfo reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII.

127. Plaintiff Sarfo does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

128. Plaintiff Sarfo received a Notice of Data Breach directly from Defendant. Thus, on information and belief, Plaintiff Sarfo's PII has already been published—or will be published

[25] *See Data Security Breach Reports*, ATTY GEN TEXAS (May 3, 2024) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (listing the types of information affected by Panda's Data Breach).

imminently—by cybercriminals on the Dark Web.

129. Through its Data Breach, Defendant compromised Plaintiff Sarfo's PII. And upon information and belief, many types of Plaintiff Sarfo's PII were compromised in the Data Breach—given that Defendant's disclosure to the Texas Attorney General revealed that an extremely broad range of PII was exposed.

130. Plaintiff Sarfo has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff Sarfo to take those steps in its breach notice.

131. Specifically, Plaintiff Sarfo has spent approximately 20–24 hours, *inter alia*:

a. placing a credit freeze on her account;

b. calling her bank to inform them about the Data Breach and asking them to check her account for any suspicious activity;

c. researching the Data Breach to determine the extent of her exposure; and

d. carefully reviewing her accounts for suspicious activity.

132. And in the aftermath of the Data Breach, Plaintiff Sarfo has suffered from a spike in spam and scam text messages and phone calls.

133. Plaintiff Sarfo fears for her personal financial security and worries about what information was exposed in the Data Breach. And because of Defendant's Data Breach, Plaintiff Sarfo has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Sarfo's injuries are precisely the type of injuries that the law contemplates and addresses.

134. Plaintiff Sarfo suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

135. Plaintiff Sarfo suffered actual injury in the form of damages to and diminution in

the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

136. Plaintiff Sarfo suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Sarfo's PII right in the hands of criminals.

137. Because of the Data Breach, Plaintiff Sarfo anticipates spending considerable amounts of time and money to try and mitigate her injuries.

138. Today, Plaintiff Sarfo has a continuing interest in ensuring that her PII—which, upon information and belief, remains insecurely backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Davis's Experiences and Injuries

139. Plaintiff Silas Davis is a natural person and citizen of Ohio. He lives in Finley, Ohio, where he intends to remain.

140. Plaintiff Davis is a current employee of Defendant—having started working for Defendant in 2024. Thus, Defendant obtained and maintained Plaintiff Davis's PII. And as a result, Plaintiff Davis was injured by Defendant's Data Breach.

141. Upon information and belief, the PII that Defendant obtained and maintained includes Plaintiff Davis's name, date of birth, address, Social Security number, driver's license number, government ID number, passport number, state ID number, financial information, financial account number, credit card number, debit card number, health insurance information, and/or medical information.[26]

142. As a condition of his employment with Defendant, Plaintiff Davis provided

[26] *See Data Security Breach Reports*, ATTY GEN TEXAS (May 3, 2024) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (listing the types of information affected by Panda's Data Breach).

Defendant with his PII. Defendant used that PII to facilitate its employment of Plaintiff Davis, including payroll, and required Plaintiff Davis to provide that PII in order to obtain employment and payment for that employment.

143. Plaintiff Davis highly values the privacy of his PII. As such, he is careful to make sure that his PII remains private and secure. And Plaintiff Davis does not knowingly disclose his PII in an unsecure manner over the internet or otherwise. Thus, he would not have disclosed his PII to Defendant if Defendant was forthcoming about its inadequate data security.

144. Plaintiff Davis provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Davis's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

145. Plaintiff Davis reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII.

146. Plaintiff Davis does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

147. Plaintiff Davis received a Notice of Data Breach in the mail directly from Defendant. Thus, on information and belief, Plaintiff Davis's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

148. Through its Data Breach, Defendant compromised Plaintiff Davis's PII. And upon information and belief, many types of Plaintiff Davis's PII were compromised in the Data Breach—given that Defendant's disclosure to the Texas Attorney General revealed that an extremely broad range of PII was exposed.

149. Plaintiff Davis has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed

Plaintiff Davis to take those steps in its breach notice.

150. Specifically, Plaintiff Davis has spent approximately 15 hours *inter alia*:

a. researching the Data Breach to determine the extent of his exposure;

b. carefully reviewing his accounts for suspicious activity;

c. changing the passwords on his various accounts; and

d. contacting his bank and putting fraud detection measures in place.

151. And in the aftermath of the Data Breach, Plaintiff Davis has suffered from a spike in spam and scam including:

a. scam emails purportedly about investments and cryptocurrencies (these began right after the Data Breach);

b. scam phone calls; and

c. scam texts purportedly related to medical appointments and a letter purportedly from a medical facility (which Plaintiff Davis does not recognize).

152. Plaintiff Davis fears for his personal financial security and worries about what information was exposed in the Data Breach. And because of Defendant's Data Breach, Plaintiff Davis has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Davis's injuries are precisely the type of injuries that the law contemplates and addresses.

153. In fact, the anxiety caused by the Data Breach was so severe that on one occasion, Plaintiff Davis became nauseous and physically ill (i.e., vomit).

154. Plaintiff suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

155. Plaintiff Davis suffered actual injury in the form of damages to and diminution in

the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

156. Plaintiff Davis suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Davis's PII right in the hands of criminals.

157. Because of the Data Breach, Plaintiff Davis anticipates spending considerable amounts of time and money to try and mitigate his injuries.

158. Today, Plaintiff Davis has a continuing interest in ensuring that his PII—which, upon information and belief, remains insecurely backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Oluwalowo's Experiences and Injuries

159. Plaintiff Joshua Oluwalowo is a natural person and citizen of Minnesota. He lives in Brooklyn Park, Minnesota, where he intends to remain.

160. Plaintiff Oluwalowo is a former employee of Defendant—having worked for Defendant from approximately 2020 until 2022. Thus, Defendant obtained and maintained Plaintiff Oluwalowo's PII. And as a result, Plaintiff Oluwalowo was injured by Defendant's Data Breach.

161. Upon information and belief, the PII that Defendant obtained and maintained includes Plaintiff Oluwalowo's name, date of birth, address, Social Security number, driver's license number, government ID number, passport number, state ID number, financial information, financial account number, credit card number, debit card number, health insurance information, and/or medical information.[27]

[27] *See Data Security Breach Reports*, ATTY GEN TEXAS (May 3, 2024) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (listing the types of information affected by Panda's Data Breach).

162. As a condition of his employment with Defendant, Plaintiff Oluwalowo provided Defendant with his PII. Defendant used that PII to facilitate its employment of Plaintiff Oluwalowo, including payroll, and required Plaintiff Oluwalowo to provide that PII in order to obtain employment and payment for that employment.

163. Plaintiff Oluwalowo highly values the privacy of his PII. As such, he is careful to make sure that his PII remains private and secure. And Plaintiff Oluwalowo does not knowingly disclose his PII in an unsecure manner over the internet or otherwise. Thus, he would not have disclosed his PII to Defendant if Defendant was forthcoming about its inadequate data security.

164. Plaintiff Oluwalowo provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Oluwalowo's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

165. Plaintiff Oluwalowo reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII.

166. Plaintiff Oluwalowo does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

167. Plaintiff Oluwalowo received a Notice of Data Breach in the mail directly from Defendant. Thus, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

168. Through its Data Breach, Defendant compromised Plaintiff Oluwalowo's PII. And upon information and belief, many types of Plaintiff Oluwalowo's PII were compromised in the Data Breach—given that Defendant's disclosure to the Texas Attorney General revealed that an extremely broad range of PII was exposed.

169. Plaintiff Oluwalowo has spent—and will continue to spend—significant time and

effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Oluwalowo to take those steps in its breach notice.

170. Specifically, Plaintiff Oluwalowo now reviews his various accounts every day (or every other day) since learning about his exposure in the Data Breach.

171. And in the aftermath of the Data Breach, Plaintiff Oluwalowo has suffered from a spike in spam and scam text messages.

172. Plaintiff Oluwalowo fears for his personal financial security and worries about what information was exposed in the Data Breach. And because of Defendant's Data Breach, Plaintiff Oluwalowo has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Oluwalowo's injuries are precisely the type of injuries that the law contemplates and addresses.

173. Plaintiff Oluwalowo suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

174. Plaintiff Oluwalowo suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

175. Plaintiff Oluwalowo suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Oluwalowo's PII right in the hands of criminals.

176. Because of the Data Breach, Plaintiff Oluwalowo anticipates spending considerable amounts of time and money to try and mitigate his injuries.

177. Today, Plaintiff Oluwalowo has a continuing interest in ensuring that his PII—which, upon information and belief, remains insecurely backed up in Defendant's possession—is

protected and safeguarded from additional breaches.

Plaintiff Klepper's Experiences and Injuries

178. Plaintiff Matthew Klepper is a natural person and citizen of Tennessee. He lives in Kingsport, Tennessee, where he intends to remain.

179. Plaintiff Klepper is a former employee of Defendant. Thus, Defendant obtained and maintained Plaintiff Klepper's PII. And as a result, Plaintiff Klepper was injured by Defendant's Data Breach.

180. Upon information and belief, the PII that Defendant obtained and maintained includes Plaintiff Klepper's name, date of birth, address, Social Security number, driver's license number, government ID number, passport number, state ID number, financial information, financial account number, credit card number, debit card number, health insurance information, and/or medical information.[28]

181. As a condition of his employment with Defendant, Plaintiff Klepper provided Defendant with his PII. Defendant used that PII to facilitate its employment of Plaintiff Klepper, including payroll, and required Plaintiff Klepper to provide that PII in order to obtain employment and payment for that employment.

182. Plaintiff Klepper highly values the privacy of his PII. As such, he is careful to make sure that his PII remains private and secure. And Plaintiff Klepper does not knowingly disclose his PII in an unsecure manner over the internet or otherwise. Thus, he would not have disclosed his PII to Defendant if Defendant was forthcoming about its inadequate data security.

183. Plaintiff Klepper provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and

[28] *See Data Security Breach Reports*, ATTY GEN TEXAS (May 3, 2024) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (listing the types of information affected by Panda's Data Breach).

federal law. Defendant obtained and continues to maintain Plaintiff Klepper's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

184. Plaintiff Klepper reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII.

185. Plaintiff Klepper does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

186. Plaintiff Klepper received a Notice of Data Breach in the mail directly from Defendant. Thus, on information and belief, Plaintiff Klepper's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

187. Through its Data Breach, Defendant compromised Plaintiff Klepper's PII. And upon information and belief, many types of Plaintiff Klepper's PII were compromised in the Data Breach—given that Defendant's disclosure to the Texas Attorney General revealed that an extremely broad range of PII was exposed.

188. Plaintiff Klepper has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Klepper to take those steps in its breach notice.

189. And in the aftermath of the Data Breach, Plaintiff Klepper has suffered from a spike in spam and scam emails, text messages and phone calls—including approximately 20 scam calls per day.

190. Plaintiff Klepper fears for his personal financial security and worries about what information was exposed in the Data Breach. And because of Defendant's Data Breach, Plaintiff Klepper has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Klepper's injuries are precisely the type of injuries that the law contemplates and

addresses.

191. Plaintiff Klepper suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

192. Plaintiff Klepper suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

193. Plaintiff Klepper suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Klepper's PII right in the hands of criminals.

194. Because of the Data Breach, Plaintiff Klepper anticipates spending considerable amounts of time and money to try and mitigate his injuries. In fact, Plaintiff has already:

a. spent time resetting the automatic billing settings on his accounts; and

b. incurred approximately ***$200.00*** in late and/or declined payment fees.

195. Today, Plaintiff Klepper has a continuing interest in ensuring that his PII—which, upon information and belief, remains insecurely backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Little's Experiences and Injuries

196. Plaintiff Elizabeth Little (née Jimenez) is a natural person and citizen of Texas. She lives in Clyde, Texas, where she intends to remain.

197. Plaintiff Little is a former employee of Defendant. Thus, Defendant obtained and maintained Plaintiff Little's PII. And as a result, Plaintiff was injured by Defendant's Data Breach.

198. Upon information and belief, the PII that Defendant obtained and maintained includes Plaintiff Little's name, date of birth, address, Social Security number, driver's license

number, government ID number, passport number, state ID number, financial information, financial account number, credit card number, debit card number, health insurance information, and/or medical information.[29]

199. As a condition of her employment with Defendant, Plaintiff Little provided Defendant with her PII. Defendant used that PII to facilitate its employment of Plaintiff Little, including payroll, and required Plaintiff Little to provide that PII in order to obtain employment and payment for that employment.

200. Plaintiff Little highly values the privacy of her PII. As such, she is careful to make sure that her PII remains private and secure. And Plaintiff Little does not knowingly disclose her PII in an unsecure manner over the internet or otherwise. Thus, she would not have disclosed her PII to Defendant if Defendant was forthcoming about its inadequate data security.

201. Plaintiff Little provided her PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Little's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

202. Plaintiff Little reasonably understood that a portion of the funds derived from her employment would be used to pay for adequate cybersecurity and protection of PII.

203. Plaintiff Little does not recall ever learning that her information was compromised in a data breach incident—other than the breach at issue here.

204. Plaintiff Little received a Notice of Data Breach from Defendant in the mail. Thus, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

[29] *See Data Security Breach Reports*, ATTY GEN TEXAS (May 3, 2024) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (listing the types of information affected by Panda's Data Breach).

205. Through its Data Breach, Defendant compromised Plaintiff Little's PII. And upon information and belief, many types of Plaintiff Little's PII were compromised in the Data Breach—given that Defendant's disclosure to the Texas Attorney General revealed that an extremely broad range of PII was exposed.

206. Plaintiff has ***already*** suffered from identity theft and fraud:

a. in or around mid-2024, a cybercriminal stole money out of her bank account (as a result, the bank froze her account);

b. her "CashApp" account was subjected to a fraudulent charge attempt;

c. her credit was subjected to fraudulent inquiries (e.g., with "Amazon" and for a credit account).

207. Moreover, in or around March–April 2024, Plaintiff Little was notified that her PII was found ***published*** on the Dark Web.

208. Plaintiff Little has spent—and will continue to spend—significant time and effort monitoring her accounts to protect herself from identity theft. After all, Defendant directed Plaintiff Little to take those steps in its breach notice.

209. Specifically, Plaintiff Little has spent 4-6 hours, *inter alia*:

a. researching the Data Breach to determine the extent of her exposure;

b. carefully reviewing her accounts for suspicious activity (e.g., she has checked her credit daily for several weeks using "Credit Karma" and "WalletHub");

c. talking to her bank over the phone about the suspicious activity; and

d. traveling 40–50 miles to her bank to address the suspicious activity.

210. And in the aftermath of the Data Breach, Plaintiff Little has suffered from a spike in spam and scam phone calls.

211. Plaintiff Little fears for her personal financial security and worries about what information was exposed in the Data Breach. And because of Defendant's Data Breach, Plaintiff Little has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Little's injuries are precisely the type of injuries that the law contemplates and addresses.

212. Plaintiff Little suffered actual injury from the exposure and theft of her PII—which violates her rights to privacy.

213. Plaintiff Little suffered actual injury in the form of damages to and diminution in the value of her PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

214. Plaintiff Little suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff Little's PII right in the hands of criminals.

215. Because of the Data Breach, Plaintiff Little anticipates spending considerable amounts of time and money to try and mitigate her injuries.

216. Today, Plaintiff Little has a continuing interest in ensuring that her PII—which, upon information and belief, remains insecurely backed up in Defendant's possession—is protected and safeguarded from additional breaches.

Plaintiff Jackson's Experiences and Injuries

217. Plaintiff Steven Jackson is a natural person and citizen of Utah. He lives in Saratoga Springs, Utah, where he intends to remain.

218. Plaintiff Jackson is a former employee of Defendant. Thus, Defendant obtained and maintained Plaintiff Jackson's PII. And as a result, Plaintiff Jackson was injured by Defendant's Data Breach.

219. Upon information and belief, the PII that Defendant obtained and maintained includes Plaintiff Jackson's name, date of birth, address, Social Security number, driver's license number, government ID number, passport number, state ID number, financial information, financial account number, credit card number, debit card number, health insurance information, and/or medical information.[30]

220. As a condition of his employment with Defendant, Plaintiff Jackson provided Defendant with his PII. Defendant used that PII to facilitate its employment of Plaintiff Jackson, including payroll, and required Plaintiff Jackson to provide that PII in order to obtain employment and payment for that employment.

221. Plaintiff Jackson highly values the privacy of his PII. As such, he is careful to make sure that his PII remains private and secure. And Plaintiff Jackson does not knowingly disclose his PII in an unsecure manner over the internet or otherwise. Thus, he would not have disclosed his PII to Defendant if Defendant was forthcoming about its inadequate data security.

222. Plaintiff Jackson provided his PII to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff Jackson's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure.

223. Plaintiff Jackson reasonably understood that a portion of the funds derived from his employment would be used to pay for adequate cybersecurity and protection of PII.

224. Plaintiff Jackson does not recall ever learning that his information was compromised in a data breach incident—other than the breach at issue here.

225. Plaintiff Jackson received a Notice of Data Breach letter directly from Defendant.

[30] *See Data Security Breach Reports*, ATTY GEN TEXAS (May 3, 2024) https://oag.my.site.com/datasecuritybreachreport/apex/DataSecurityReportsPage (listing the types of information affected by Panda's Data Breach).

Thus, on information and belief, Plaintiff's PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

226. Through its Data Breach, Defendant compromised Plaintiff Jackson's PII. And upon information and belief, many types of Plaintiff Jackson's PII were compromised in the Data Breach—given that Defendant's disclosure to the Texas Attorney General revealed that an extremely broad range of PII was exposed.

227. Plaintiff Jackson has ***already*** suffered from identity theft and fraud:

a. an identity thief fraudulently applied for a credit card in his name; and

b. his bank account was subjected to a fraudulent charge in or around March 2024.

c. Critically, Plaintiff Jackson suffered numerous other injuries resulting from the fraudulent charge on his bank account. Specifically:

d. Plaintiff Jackson was forced to close and then reopen his bank account;

e. Plaintiff Jackson incurred an "overdraft fee" due to the closing and reopening of his account; and

f. Plaintiff Jackson was forced to pay a "late rent fee" of approximately ***$250.00*** (the issues with Plaintiff's bank account resulted in a late rent payment).

228. Plaintiff Jackson has spent—and will continue to spend—significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff Jackson to take those steps in its breach notice.

229. Specifically, Plaintiff Jackson has spent approximately 10 hours, *inter alia*:

a. researching his legal rights as a data breach victim;

b. verifying Defendant's breach notice and researching the Data Breach;

c. changing the passwords on his various accounts;

d. reviewing his various accounts for suspicious activity;

e. signing up for credit monitoring; and

f. communicating with his bank to open and close his account (due to the fraudulent charge).

230. Moreover, Plaintiff Jackson was warned that his PII—including his email and phone number—were ***published*** on the Dark Web. Upon information and belief, a broad range of Plaintiff Jackson's PII was published on the Dark Web because of the severity of Defendant's Data Breach.

231. And in the aftermath of the Data Breach, Plaintiff Jackson has suffered from a spike in spam and scam text messages and phone calls.

232. Plaintiff Jackson fears for his personal financial security and worries about what information was exposed in the Data Breach. And because of Defendant's Data Breach, Plaintiff Jackson has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff Jackson's injuries are precisely the type of injuries that the law contemplates and addresses.

233. Plaintiff Jackson suffered actual injury from the exposure and theft of his PII—which violates his rights to privacy.

234. Plaintiff Jackson suffered actual injury in the form of damages to and diminution in the value of his PII. After all, PII is a form of intangible property—property that Defendant was required to adequately protect.

235. Plaintiff Jackson suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data

Breach placed Plaintiff Jackson's PII right in the hands of criminals.

236. Because of the Data Breach, Plaintiff Jackson anticipates spending considerable amounts of time and money to try and mitigate his injuries.

237. Today, Plaintiff Jackson has a continuing interest in ensuring that his PII—which, upon information and belief, remains insecurely backed up in Defendant's possession—is protected and safeguarded from additional breaches.

CLASS ACTION ALLEGATIONS

238. Plaintiffs bring this action on behalf of himself and all other similarly situated persons pursuant to California Code of Civil Procedure § 382. Plaintiffs seek to represent the following class:

> **All residents of the United States whose personal information was compromised in or as a result of the data breach of Panda Restaurant Group, Inc. announced on or around April 2024.**

239. Excluded from the class are the following individuals and/or entities: Defendant and its parents, subsidiaries, affiliates, officers, directors, or employees, and any entity in which Defendant 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.

240. Plaintiffs reserve the right to amend or modify the class definition with greater particularity or further division into subclasses or limitation to particular issues.

241. This action has been brought and may be maintained as a class action under California Code of Civil Procedure § 382 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, Plaintiffs believe the cybersecurity breach affected thousands of individuals around the country.

b. Commonality: There are questions of law and fact common to Plaintiffs 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 Panda owed a duty to Plaintiffs and Class Members to exercise due care in collecting, storing, processing, and safeguarding their personal information;

ii. Whether Panda breached those duties;

iii. Whether Panda implemented and maintained reasonable security procedures and practices appropriate to the nature of the personal information of Class Members;

iv. Whether Panda acted negligently in connection with the monitoring and/or protecting of Plaintiffs' and Class Members' personal information;

v. Whether Panda knew or should have known that they did not employ reasonable measures to keep Plaintiffs' and Class Members' personal information secure and prevent loss or misuse of that personal information;

vi. Whether Panda adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

vii. Whether Panda caused Plaintiffs and Class Members damages;

viii. Whether the damages Panda caused to Plaintiffs 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 Panda violated the law by failing to promptly notify Class Members that their personal information had been compromised;

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

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

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

xiii. Whether Panda'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); and

xiv. Whether Panda's failure to implement and maintain reasonable security procedures and practices constitutes violation of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150, California's Unfair Competition Law, Cal. Bus. & Prof. Code § 17200.

c. Typicality. The claims of the named Plaintiffs are typical of the claims of the Class Members because all had their personal information compromised as a result of Panda's failure to implement and maintain reasonable security measures and the consequent Data Breach.

d. Adequacy of Representation. Plaintiffs will fairly and adequately represent the interests of the Class. Counsel who represent Plaintiffs 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 a single Plaintiff. Each Plaintiff has been damaged and is entitled to recovery by reason of Defendant'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 Defendant's records will readily enable the Court and parties to ascertain affected companies and their employees.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

242. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

243. Plaintiffs and the Class (or their third-party agents) entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their PII, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

244. Defendant owed a duty of care to Plaintiffs and Class Members because it was foreseeable that Defendant's failure to use adequate data security in accordance with industry standards for data security would compromise their PII in a data breach. And here, that foreseeable danger came to pass.

245. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Class could and would suffer if their PII was wrongfully disclosed.

246. Defendant owed these duties to Plaintiffs and Class Members 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 practices. After all, Defendant actively sought and obtained Plaintiffs and Class Members' PII.

247. Defendant owed to Plaintiffs and Class Members at least the following duties to:

a. exercise reasonable care in handling and using the PII in its care and custody;

b. implement industry-standard security procedures sufficient to reasonably protect the information from a data breach, theft, and unauthorized access;

c. promptly detect attempts at unauthorized access;

d. notify Plaintiffs and Class Members within a reasonable timeframe of any breach to the security of their PII.

248. Thus, Defendant owed a duty to timely and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the Data Breach. After all, this duty is required and necessary for Plaintiffs and Class Members 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.

249. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain under applicable regulations.

250. Defendant knew or reasonably should have known that the failure to exercise due care in the collection, storage, and use of the PII of Plaintiffs and the Class involved an

unreasonable risk of harm to Plaintiffs and the Class, even if the harm occurred through the criminal acts of a third party.

251. Defendant's duty to use reasonable security measures arose because of the special relationship that existed between Defendant and Plaintiffs and the Class. That special relationship arose because Plaintiffs and the Class (or their third-party agents) entrusted Defendant with their confidential PII, a necessary part of obtaining employment from Defendant.

252. 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.

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

254. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

255. Defendant breached these duties as evidenced by the Data Breach.

256. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and Class Members' PII by:

a. disclosing and providing access to this information to third parties; and

b. failing to properly supervise the way the PII was stored, used, and exchanged, and those in its employ who were responsible for making that happen.

257. Defendant breached its duties by failing to exercise reasonable care in supervising its agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and Class Members which actually and proximately caused the Data Breach and Plaintiffs' and Class Members' injury.

258. Defendant further breached its duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and Class Members, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs' and Class Members' injuries-in-fact.

259. Defendant has admitted that the PII of Plaintiffs and the Class was wrongfully lost and disclosed to unauthorized third persons because of the Data Breach.

260. As a direct and traceable result of Defendant's negligence and/or negligent supervision, Plaintiffs and Class Members have suffered and will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

261. On information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

262. Defendant's breach of its common-law duties to exercise reasonable care and its failures and negligence actually and proximately caused Plaintiffs and Class Members 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.

SECOND CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

263. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

264. Plaintiffs and Class Members either directly contracted with Defendant or Plaintiffs and Class Members were the third-party beneficiaries of contracts with Defendant.

265. Plaintiffs and Class Members were required to provide their PII to Defendant as a condition of employment with Defendant. Plaintiffs and Class Members provided their PII to Defendant.

266. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

267. Plaintiffs and the Class Members accepted Defendant's offers by disclosing their PII to Defendant or its third-party agents in exchange for employment.

268. In turn, and through internal policies, Defendant agreed to protect and not disclose the PII to unauthorized persons.

269. In its Privacy Policy, Defendant represented that they had a legal duty to protect Plaintiffs' and Class Members' PII.

270. Implicit in the parties' agreement was that Defendant would provide Plaintiffs and Class Members with prompt and adequate notice of all unauthorized access and/or theft of their PII.

271. After all, Plaintiffs and Class Members would not have entrusted their PII to Defendant in the absence of such an agreement with Defendant.

272. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

273. The covenant of good faith and fair dealing is an element of every contract. Thus, parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—and not merely the letter—of the bargain. In short, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to its form.

274. Subterfuge and evasion violate the duty of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or consist of inaction. And fair dealing may require more than honesty.

275. Defendant materially breached the contracts it entered with Plaintiffs and Class Members by:

a. failing to safeguard their information;

b. failing to notify them promptly of the intrusion into its computer systems that compromised such information;

c. failing to comply with industry standards;

d. failing to comply with the legal obligations necessarily incorporated into the agreements; and

e. failing to ensure the confidentiality and integrity of the electronic PII that Defendant created, received, maintained, and transmitted.

276. In these and other ways, Defendant violated its duty of good faith and fair dealing.

277. Defendant's material breaches were the direct and proximate cause of Plaintiffs' and Class Members' injuries (as detailed *supra*).

278. And, on information and belief, Plaintiffs' PII has already been published—or will be published imminently—by cybercriminals on the Dark Web.

279. Plaintiffs and Class Members performed as required under the relevant agreements, or such performance was waived by Defendant's conduct.

THIRD CAUSE OF ACTION
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

280. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

281. This claim is pleaded in the alternative to the breach of implied contract claim.

282. Plaintiffs and Class Members conferred a benefit upon Defendant. After all, Defendant benefitted from using their PII to facilitate its business.

283. Defendant appreciated or had knowledge of the benefits it received from Plaintiffs and Class Members.

284. Plaintiffs and Class Members reasonably understood that Defendant would use adequate cybersecurity measures to protect the PII that they were required to provide based on Defendant's duties under state and federal law and its internal policies.

285. Defendant enriched itself by saving the costs they reasonably should have expended on data security measures to secure Plaintiffs' and Class Members' PII.

286. Instead of providing a reasonable level of security, or retention policies, that would have prevented the Data Breach, Defendant instead calculated to avoid its data security obligations at the expense of Plaintiffs and Class Members by utilizing cheaper, ineffective security measures. Plaintiffs and Class Members suffered as a direct and proximate result of Defendant's failure to provide the requisite security.

287. Under principles of equity and good conscience, Defendant should not be permitted to retain the full value of Plaintiffs' and Class Members' payment and/or PII because Defendant failed to adequately protect their PII.

288. Plaintiffs and Class Members have no adequate remedy at law.

289. Defendant should be compelled to disgorge into a common fund—for the benefit of Plaintiffs and Class Members—all unlawful or inequitable proceeds that it received because of its misconduct.

FOURTH CAUSE OF ACTION
Violation of the California Consumer Privacy Act,
Cal. Civ. Code §§ 1798.100 *et seq.*, § 1798.150
(On Behalf of Plaintiffs and the Class)

290. Plaintiffs reallege and incorporates by reference the preceding paragraphs as though fully set forth herein.

291. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

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

292. Panda is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

293. Plaintiffs and Class Members are covered "consumers" under § 1798.140(g) in

that they are natural persons, many of who are California residents.

294. The personal information of Plaintiffs and Class Members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Panda collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

295. Panda knew or should have known that its computer systems and data security practices were inadequate to safeguard the Plaintiffs' and Class Members' personal information and that the risk of a data breach or theft was highly likely. Panda failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiffs and the Class. Specifically, Panda subjected Plaintiffs' and Class Members' nonencrypted and nonredacted personal information to an unauthorized access and exfiltration, theft, or disclosure as a result of the Panda's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

296. As a direct and proximate result of Panda's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and Class Members' personal information included exfiltration, theft, or disclosure through Panda's servers, systems, and website, and/or the dark web, where hackers further disclosed Panda's customers' and their

employees' personal information.

297. As a direct and proximate result of Panda's acts, Plaintiffs and Class Members were injured and lost money or property, the loss of Plaintiffs' and the Class's legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

298. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages." Accordingly, Plaintiffs and the Class by way of this complaint seek actual pecuniary damages suffered as a result of Panda's violations described herein. Plaintiffs have issued and/or will issue a notice of these alleged violations pursuant to § 1798.150(b) and intends to amend this complaint to seek statutory damages and injunctive relief upon expiration of the 30-day cure period pursuant to § 1798(a)(1)(A)-(B), (a)(2), and (b).

FIFTH CAUSE OF ACTION
Violation of the California Unfair Competition Law, Cal. Bus. & Prof. Code §17200 *et seq.*
(On Behalf of Plaintiffs and the Class)

299. Plaintiffs reallege and incorporate by reference the preceding paragraphs as though fully set forth herein.

300. Panda is a "person" defined by Cal. Bus. & Prof. Code § 17201.

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

302. Panda's "unfair" acts and practices include:

a. Panda failed to implement and maintain reasonable security measures to protect Plaintiffs' and Class Members' personal information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Panda data breach. Panda 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. Panda'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. Panda'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 Panda's inadequate security, consumers could not have reasonably avoided the harms that Panda caused.

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

303. Panda 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.

304. Panda's unlawful, unfair, and deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class Members' personal information, which was a direct and proximate cause of the Panda 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 Panda data breach;

c. Failing to comply with common law and statutory duties pertaining to the

security and privacy of Plaintiffs' and Class 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 Panda data breach.

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class 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 Plaintiffs' and Class 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 Plaintiffs' and Class 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 Plaintiffs' and Class 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.

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

306. As a direct and proximate result of Panda's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and Class 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, and well as the time and expense of finding alternative methods of timekeeping and payroll services.

307. Panda's violations were, and are, willful, deceptive, unfair, and unconscionable.

308. Plaintiffs and Class Members have lost money and property as a result of Panda's conduct in violation of the UCL, as stated herein and above.

309. By deceptively storing, collecting, and disclosing their personal information, Panda has taken money or property from Plaintiffs and Class Members.

310. Panda acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and Class Members' rights. Past data breaches put it on notice that its security and privacy protections were inadequate.

311. Plaintiffs and Class Members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Panda'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.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, pray for the following relief:

1. An order certifying the class pursuant to California Code of Civil Procedure § 382 and declaring that Plaintiffs are the class representatives and appointing Plaintiffs' counsel as class counsel;
2. Permanent injunctive relief to prohibit Panda 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;
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. A declaration of right and liabilities of the parties;

7. Costs of suit;

8. Reasonable attorneys' fees, including pursuant to Cal. Civ. Pro. Code § 1021.5;

9. Pre- and post-judgment interest at the maximum legal rate;

10. 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

11. Such other relief as the Court deems just and proper.

Dated: April 23, 2025

WUCETICH & KOROVILAS LLP

By: 

Jason M. Wucetich
Attorneys for Plaintiffs,
individually and on behalf of
all others similarly situated

Daniel Srourian, Esq.
SROURIAN LAW FIRM, P.C.
3435 Wilshire Blvd., Suite 1710
Los Angeles, California 90010
T: (213) 474-3800
F: (213) 471-4160
daniel@slfla.com

John J. Nelson
MILBERG COLEMAN BRYSON PHILLIPSGROSSMAN PLLC
280 South Beverly Drive
Beverly Hills, California 90212
T: (858) 209-6941
jnelson@milberg.com

Todd S. Garber*
FINKELSTEIN BLANKINSHIP FREI-PEARSON AND GARBER LLP
1 North Broadway, Suite 900
White Plains, New York 10601
T: (914) 298-3283
tgarber@fbfglaw.com

Bassma Zebib
LAW OFFICE OF BASSMA ZEBIB
8616 La Tijera Boulevard Suite 303
Los Angeles, California 90045
T: (323) 406-0666
bassma@zebiblaw.com

Paul M. De Marco
MARKOVITS, STOCK AND DEMARCO, LLC
119 East Court Street, Suite 530
Cincinnati, Ohio 45202
T: (513) 651-3700
pdemarco@msdlegal.com

Bryan L Bleichner
CHESTNUT CAMBRONNE PA
100 Washington Avenue Suite 1700
Minneapolis, Minnesota 55401
T: (612) 339-7300
bbleichner@chestnutcambronne.com

Kristen Lake Cardoso
KOPELOWITZ OSTROW PA
One West Las Olas Boulevard, Suite 500
Fort Lauderdale, Florida 33301
T: (954) 525-4100
cardoso@kolawyers.com

Kevin Laukaitis*
LAUKAITIS LAW LLC
954 Avenida Ponce De Leon,
Suite 205, No. 10518
San Juan, Puerto Rico 00907
T: (215) 789-4462
klaukaitis@laukaitislaw.com

Andrew Gerald Gunem
STRAUSS BORRELLI PLLC
980 North Michigan Avenue, Suite 1610

Chicago, Illinois 60611
T: (872) 263-1100
agunem@straussborrelli.com

Counsel for Representative Plaintiffs and the Proposed Class(es)

DEMAND FOR JURY TRIAL

Plaintiffs, on behalf of themselves and the class, hereby demand a trial by jury on all issues of fact or law so triable.

Dated: April 23, 2025

WUCETICH & KOROVILAS LLP

By: 

Jason M. Wucetich
Attorneys for Plaintiffs,
individually and on behalf of
all others similarly situated

PROOF OF SERVICE

I am more than eighteen years old and not a party to this action. My business address is Wucetich & Korovilas LLP, 222 North Sepulveda Boulevard, Suite 2000, El Segundo, California 90245.

On April 23, 2025 I served the following document(s):

- AMENDED CLASS ACTION COMPLAINT

on the interested parties in this action by placing a true and correct copy or copies thereof in sealed envelope(s) addressed as follows:

Marcus McCutcheon (SBN 281444)
BAKER & HOSTETLER LLP
600 Anton Boulevard Suite 900
Costa Mesa, CA 92626-7221
Telephone: 714.754.6600
Facsimile: 714.754.6611

Counsel for Defendant Panda Restaurant Group, Inc.

I deposited such envelope(s) with postage thereon fully prepaid in the United States mail at a facility regularly maintained by the United States Postal Service at El Segundo, California, on the date indicated above.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this 23rd day of April 2025, at El Segundo, California.

Jason M. Wucetich