BRADLEY/GROMBACHER, LLP
Marcus J. Bradley, Esq. (SBN 174156)
Kiley L. Grombacher, Esq. (SBN 245960)
Lirit A. King, Esq. (SBN 252521)
31365 Oak Crest Drive, Suite 240
Westlake Village, California 91361
Telephone: (805) 270-7100
Facsimile: (805) 270-7589
E-Mail: mbradley@bradleygrombacher.com
kgrombacher@bradleygrombacher.com
lking@bradleygrombacher.com

AYLSTOCK, WITKIN, KREIS & OVERHOLTZ, PLLC
Bryan F. Aylstock, *pro hac vice pending*
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: (850) 202-1010
Facsimile: (850) 916-7449
Email: baylstock@awkolaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

TAMMY GUTIERREZ, an individual, and on behalf of classes of similarly situated individuals,

Plaintiff,

v.

SAMSUNG ELECTRONICS AMERICA, INC., a New York corporation,

Defendant.

CASE NO:

CLASS ACTION COMPLAINT FOR:

1. **NEGLIGENCE;**
2. **UNJUST ENRICHMENT;**
3. **BREACH OF EXPRESS CONTRACT;**
4. **BREACH OF IMPLIED CONTRACT;**
5. **INVASION OF PRIVACY; AND**
6. **VIOLATION OF THE CALIFORNIA CONSUMER PRIVACY ACT § 1798.150.**

DEMAND FOR A JURY TRIAL

Plaintiff Tammy Gutierrez ("Plaintiff") brings this Class Action Complaint against Samsung Electronics America, Inc. ("Defendant" or "Samsung"), in her individual capacity and on behalf of all others similarly situated, and alleges, upon personal knowledge as to her own actions and her counsels' investigations, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. This is a class action for damages with respect to Defendant Samsung Electronics America, Inc. and its failure to exercise reasonable care in securing sensitive personal information including without limitation, unencrypted and unredacted name, contact and demographic information, and date of birth (collectively, "personal identifiable information" or "PII").

2. Plaintiff seeks damages for herself and other similarly situated current and former student loan borrowers ("borrowers"), or any other person(s) impacted in the data breach at issue ("Class Members"), as well as other equitable relief, including, without limitation, injunctive relief designed to protect the very sensitive information of Plaintiff and other Class Members.

3. On or about September 2, 2022, Samsung notified Plaintiff and Class Members about a widespread data breach involving sensitive PII. The number of individuals affected has not been disclosed by Samsung, however, because Samsung is one of the largest technology companies, the breach could have involved hundreds of millions of users. Samsung explained in the notice email that it discovered an unauthorized third-party gained access to a portion of Samsung's system. Samsung discovered that files on its network were accessed and acquired by the unauthorized actor (the "Data Breach").

4. Plaintiff and the Class Members in this action were, upon information and belief, current and former Samsung users with their PII on Samsung's system. Upon information and belief, the first that Plaintiff and the Class Members learned of the Data Breach was when they received by email Notice of Data Breach letters

on or about September 2, 2022.

5. The Data Breach affected individuals whose information was stored on Defendant's servers in multiple states.

6. In this era of frequent data security attacks and data breaches, particularly in the technology industry, Defendant's failures leading to the Data Breach are particularly egregious, as this Data Breach was highly foreseeable.

7. Defendant reported to Plaintiff Tammy Gutierrez that information compromised in the Data Breach included her PII.

8. Upon information and belief, Plaintiff's and Class Members' PII was unencrypted and unredacted PII and was compromised due to Samsung's negligent and/or careless acts and omissions.

9. Upon information and belief, based on the type of sophisticated and malicious criminal activity, the type of PII targeted, Defendant's admission that the PII was accessed, Defendant's admission that Plaintiff and Class Member's PII was in the files that were accessed, reports of criminal misuse of Plaintiff's and Class Members' data, and reports of PII on the Dark Web following the Data Breach, Plaintiff's and Class Members' PII was likely accessed, disclosed, exfiltrated, stolen, disseminated, and used by a criminal third party.

10. As a result of the Data Breach, Plaintiff and the Class Members are at an imminent risk of identity theft.

11. The risk of identity theft is not speculative or hypothetical but is impending and has materialized as there is evidence that Plaintiff's and Class Members' PII was targeted, accessed, and may have been disseminated on the Dark Web. Moreover, Class members have suffered actual identity theft and misuse of their data following the data breach.

12. As Defendant instructed, advised, and warned in its Security Response Webpage,[1] Plaintiff and the Class Members must now closely monitor their financial

[1] https://www.samsung.com/us/support/securityresponsecenter/ (last accessed Sept. 6, 2022)

accounts to guard against future identity theft and fraud. Plaintiff's and Class Members' have heeded such warnings to mitigate against the imminent risk of future identity theft and financial loss. Such mitigation efforts included and will include into the future: reviewing financial statements, changing passwords, and signing up for credit and identity theft monitoring services. The loss of time and other mitigation costs are tied directly to guarding against and mitigating against the imminent risk of identity theft.

13. Plaintiff and Class Members have suffered numerous actual and concrete injuries as a direct result of the Data Breach, including: (a) invasion of privacy; (b) financial costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft; (d) financial costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time heeding Defendant's warnings and following its instructions in the Notice Letter; (g) the loss of benefit of the bargain (price premium damages), to the extent Class Members paid Samsung for services; (h) deprivation of value of their PII; and (i) the continued risk to their Sensitive Information, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information.

14. Plaintiff seeks to remedy these harms, and to prevent the future occurrence of an additional data breach, on behalf of themselves and all similarly situated persons whose PII was compromised as a result of the Data Breach. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement for loss of time, reimbursement of opportunity costs, out-of-pocket costs, price premium damages, and injunctive relief including improvements to Defendant's data security systems and protocols, future annual audits, and adequate credit monitoring services funded by the Defendant.

PARTIES

15. Plaintiff Tammy Gutierrez is a resident and citizen of California, residing in Bakersfield. Ms. Gutierrez received Samsung's *An important notice regarding customer information*, on or about September 2, 2022, by e-mail.

16. Defendant Samsung Electronics America, Inc. is a Ridgefield, New Jersey based technology device company, which has a principal place of business at 85 Challenger Road, Ridgefield Park, NJ 07660.

17. Defendant Samsung Electronics America, Inc. is a wholly-owned subsidiary of Samsung Electronics Co., Ltd, a South Korean based corporation. Its principal place of business is located at 129 Samseong-ro Yeongtong-gu Gyeonggi-do 16677 Suwon-Shi, Republic of Korea.

18. All of Plaintiff's claims stated herein are asserted against Samsung and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. § 1332, the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members, (ii) there is an aggregate amount in controversy exceeding $5,000,000, exclusive of interest and costs, and (iii) there is minimal diversity because at least one Plaintiff (CA) and Defendant (NY, NJ) are citizens of different states. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. § 1367.

20. Pursuant to 28 U.S.C. § 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District: Defendant's decision making processes affecting data and privacy stem from its San Francisco offices, Defendant markets and sells products and services in this District, Defendant gains revenue and profits from doing business in this District, consumers sign up for Samsung accounts and provide Samsung with their PII in this District, Class members affected by the breach

reside in this District, Defendant has a corporate office in this District, and Defendant employs numerous people in this District, a number of whom work specifically on making decisions regarding the data privacies and handling of consumers' data.

21. Defendant is subject to personal jurisdiction in California based upon sufficient minimum contacts which exist between Defendant and California, and the decisions affecting consumers data and privacy stem from the San Francisco offices. Defendant is authorized to do and is doing business in California, Defendant advertises and solicits business in California, Defendant has a showroom store in California, and Defendant has corporate offices in California. Defendant has purposefully availed itself to the protections of California law and should reasonably expect to be hauled into court in California for harm arising out of its pervasive contacts with California.

FACTUAL ALLEGATIONS

Defendant's Promises

22. Defendant operates its business nationwide offering various types of technological products and services.

23. Plaintiff and the Class Members, as current or former Samsung users, reasonably relied (directly or indirectly) on this sophisticated technology company to keep their sensitive PII confidential; to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their PII. Borrowers, in general, demand security to safeguard their PII, especially when financial information and other sensitive PII is involved.

24. Indeed, Samsung promotes to its customer that it takes the privacy and security of PII seriously, stating, "security is a top priority."[2]

25. Defendant's Privacy Policy ("Privacy Policy") states, "[i]n this connected, digital age, accessing this information responsibly is more important than ever - clarity and integrity about its use are essential to protecting your privacy and

[2] *Id.*

securing your confidence and peace of mind. At Samsung, we prioritize protecting your information, and design our products and services according to our three fundamental Privacy Principles."[3]

26. Defendant's Privacy Policy applies to any personal information provided to Samsung and any personal information that Samsung collects from its website, affiliates, and mobile apps.[4]

27. Defendant's Privacy Policy does not permit Defendant to use and disclose Plaintiff's and Class Members' Private Information unless complying with laws or to carry out internal functions.[5]

28. The Privacy Policy further states that Samsung "maintain[s] safeguards designed to protect personal information we obtain through the Services," and further defines "Services" as "all of our Internet-connected Samsung devices and services (from mobile phones and tablets to TVs, home appliances, online services, and more).[6]

The Data Breach

29. Defendant violated its own Privacy Policy.

30. On or about September 2, 2022, Samsung notified Plaintiff and Class Members about a widespread data breach of its computer network involving the sensitive personally identifiable information of consumers.

31. The data breach occurred in "late July 2022" when an "an unauthorized third party acquired information from some of Samsung's U.S. systems."[7]

32. According to its Notice Email to Class Members, Samsung explained that on or around August 4, 2022 (over a full month earlier) it determined through an ongoing investigation that personal information of certain customers was affected.[8]

[3] https://www.samsung.com/us/privacy/ (last accessed Sept. 6, 2022)
[4] https://www.samsung.com/us/account/privacy-policy/ (last accessed Sept. 6, 2022)
[5] *Id.*
[6] *Id.*
[7] https://www.samsung.com/us/support/securityresponsecenter/ (last accessed Sept. 6, 2022)
[8] *Id.*

33. The Notice Samsung directed to be sent to Samsung users including Plaintiff and Class Members, noted unequivocally that their PII was impacted by the Data Breach.

34. Plaintiff and Class Members in this action were, upon information and belief, current and former Samsung users whose PII was utilized by Samsung for purposes of providing products and services. Plaintiff and Class Members first learned of the Data Breach when they received by email Notice of Data Breach on or about September 2, 2022.

35. Upon information and belief, the PII was not encrypted prior to the Data Breach. Samsung did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining, causing Plaintiff's and Class Members' PII to be exposed.

36. Upon information and belief, the cyberattack was expressly designed to gain access to private and confidential data, including (among other things) the PII of Plaintiff and the Class Members.

Securing PII and Preventing Breaches

37. Samsung could have prevented this Data Breach by properly encrypting or otherwise implementing policies, procedures and computer data security programs that provided the level of protection reasonably necessary for a company of this sophistication and the custodian of large amounts of PII.

38. In the course and scope of its provision of services and products, Defendant collects massive amounts of highly sensitive PII, including but not limited to, name, contact and demographic information, date of birth.

39. Collecting, maintaining, and protecting PII is vital to virtually all of Samsung's business purposes, and Defendant benefits from the acquisition, use, and storage of the PII.

40. Plaintiff and Class Members entrusted their PII to Defendant on the premise and with the understanding that Defendant would safeguard their

information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties, and/or only retain PII for necessary business purposes and for a reasonable amount of time.

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

41. It is well known that PII, including name and contact information in particular, is an invaluable commodity and a frequent target of hackers.

42. In light of recent high profile data breaches at other industry leading companies, including, Microsoft (250 million records, December 2019), Wattpad (268 million records, June 2020), Facebook (267 million users, April 2020), Estee Lauder (440 million records, January 2020), Whisper (900 million records, March 2020), and Advanced Info Service (8.3 billion records, May 2020), Samsung knew or should have known that its systems would be targeted by cybercriminals. In fact, earlier this year, Samsung was the target of a massive security breach orchestrated by the ransomware criminal enterprise "Lapsus$", which resulted in the theft of nearly 200GB of highly sensitive internal data.[9]

43. Indeed, cyberattacks against the technology industry have been common for over ten years with the FBI warning as early as 2011 that cybercriminals were "advancing their abilities to attack a system remotely" and "[o]nce a system is compromised, cyber criminals will use their accesses to obtain PII." The FBI further warned that that "the increasing sophistication of cyber criminals will no doubt lead to an escalation in cyber crime."[10]

44. Moreover, it is well known that the specific PII at issue in this case, including names and contact information in particular, is a valuable commodity and a frequent target of hackers.

/ / /

[9] Gareth Corfield, *Lapsus$ extortionists dump Samsung data online, chaebol confirms security breach*, THE REGISTER, Mar. 7, 2022, <https://www.theregister.com/2022/03/07/samsung_lapsus_data_theft/>

[10] Gordon M. Snow, *Statement before the House Financial Services Committee, Subcommittee on Financial Institutions and Consumer Credit*, FBI (Sept. 14, 2011), https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector.

45. As a sophisticated financial and lending entity that collects, utilizes, and stores particularly sensitive PII, Samsung was at all times fully aware of the increasing risks of cyber-attacks targeting the PII it controlled, and its obligation to protect the PII of Plaintiff and Class Members.

46. Defendant has acknowledged through conduct and statements that the misuse or inadvertent disclosure of PII can pose major privacy and financial risks to impacted individuals, and that under state law they may not disclose and must take reasonable steps to protect PII from improper release or disclosure.

The Value of Personal Identifiable Information

47. There is both a healthy black market and a legitimate market for the type of PII that was compromised in this action. PII is such a valuable commodity to criminal networks that once the information has been compromised, criminals often trade the information on the "cyber black market" for years.

48. The PII of consumers remains of high value to criminals, as evidenced by the prices they will pay through the Dark Web. Numerous sources cite Dark Web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.

49. According to the Dark Web Price Index for 2021, payment card details for an account balance up to $1,000 have an average market value of $150, credit card details with an account balance up to $5,000 have an average market value of $240, stolen online banking logins with a minimum of $100 on the account have an average market value of $40, and stolen online banking logins with a minimum of $2,000 on the account have an average market value of $120. Criminals can also purchase access to entire company data breaches from $900 to $4,500.

50. A dishonest person who has your name and contact information can use it to get other personal information about you. A breach including this type of information places data breach victims at an increased risk of phishing and social

engineering attacks, eventually leading to identity theft.

51. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x in price on the black market."

Defendant Failed to Comply with Recognized Security Standards

52. Despite the prevalence of public announcements of data breach and data security compromises, and despite Defendant's own acknowledgment of its duties to keep PII private and secure and its previous experience as the target of cyberattacks, Defendant failed to take appropriate steps to protect the PII of Plaintiff and the proposed Class from being compromised.

53. Samsung had the resources necessary to prevent the Data Breach but neglected to adequately invest in security measures, despite its obligation to protect such information. Accordingly, Samsung breached its common law, statutory, and other duties owed to Plaintiff and Class Members.

54. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;
b. Maintaining appropriate design, systems, and controls to limit user access to certain information as necessary;
c. Monitoring for suspicious or irregular traffic to servers;
d. Monitoring for suspicious credentials used to access servers;
e. Monitoring for suspicious or irregular activity by known users;
f. Monitoring for suspicious or unknown users;
g. Monitoring for suspicious or irregular server requests;
h. Monitoring for server requests for PII;
i. Monitoring for server requests from VPNs; and

j. Monitoring for server requests from Tor exit nodes.

55. Upon information and belief, Defendant failed to comply with one or more of these standards.

Samsung Failed to Comply with FTC Guidelines

56. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[11] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[12]

57. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making.

58. The FTC has brought well publicized enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. This includes the FTC's enforcement action against Equifax following a massive data breach involving the personal and financial information of 147 million Americans.

59. In 2016, the FTC updated its publication, "Protecting Personal Information: A Guide for Business," which established cyber-security guidelines for

[11] 17 C.F.R. § 248.201 (2013).
[12] *Id.*

businesses. There, the FTC advised that businesses should protect the PII that they keep by following some minimum standards related to data security, including, among others:

(a) Encrypting information stored on computer networks;

(b) Identifying network vulnerabilities;

(c) Implementing policies to update and correct any security problems;

(d) Utilizing an intrusion detection systems;

(e) Monitor all incoming traffic for suspicious activity indicating someone is attempting to hack the system;

(f) Watching for large amounts of data being transmitted from the system;

(g) Developing a response plan ready in the event of a breach;

(h) Limiting employee and vendor access to sensitive data;

(i) Requiting complex passwords to be used on networks;

(j) Utilizing industry-tested methods for security;

(k) Verifying that third-party service providers have implemented reasonable security measures;

(l) Educating and training employees on data security practices;

(m) Implementing multi-layer security including firewalls, anti-virus, and anti-malware software;

(n) Implementing multi-factor authentication.

60. Upon information and belief, Defendant failed to implement or adequately implement at least one of these fundamental data security practices.

61. Defendant's failure constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

/ / /

/ / /

Plaintiff and Class Members Have Suffered Concrete Injury as a Result of Defendant's Inadequate Security and the Data Breach it Allowed.

62. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the foreseeable consequences of the PII ending up in the possession of criminals, the risk of identity theft is materialized and imminent.

63. Given the type of targeted attack in this case, the sophisticated criminal activity, and the type of PII, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/Dark Web for sale and purchase by criminals intending to utilize the PII for identity theft crimes, such as opening bank accounts in the victims' names to make purchases or to launder money; file false tax returns; or file false unemployment claims.

64. Furthermore, the information accessed and disseminated in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, where victims can easily cancel or close credit and debit card accounts. The information disclosed in this Data Breach is impossible to "close" and difficult, if not impossible, to change (such as names and contact information).

65. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. The fraudulent activity resulting from the Data Breach may not become evident for years.

66. Indeed, "[t]he risk level is growing for anyone whose information is stolen in a data breach." Moreover, there is a high likelihood that significant identity fraud and/or identity theft has not yet been discovered or reported. Even data that have not yet been exploited by cybercriminals bears a high risk that the cybercriminals who now possess Class Members' PII will do so at a later date or re-sell it.

/ / /

67. To date, Defendant has done little to adequately protect Plaintiff and Class Members, or to compensate them for their injuries sustained in this data breach.

68. Thus, due to the actual and imminent risk of identity theft, Plaintiff and Class Members must, in Defendant's words, "remain vigilant" and monitor their financial accounts for many years to mitigate the risk of identity theft.

69. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as placing "freezes" and "alerts" with credit reporting agencies, contacting financial institutions, closing or modifying financial accounts, changing passwords, reviewing and monitoring credit reports and accounts for unauthorized activity, and filing police reports, which may take years to discover and detect.

70. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

71. Plaintiff's mitigation efforts are also consistent with the steps that the FTC recommends that data breach victims take to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

72. Furthermore, Defendant's poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendant or its clients for services, Plaintiff and other reasonable consumers understood and expected that they were paying for services and data security, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected.

73. As a result of Defendant's ineffective and inadequate data security and retention measures, the Data Breach, and the imminent risk of identity theft, Plaintiff and Class Members have suffered numerous actual and concrete injuries, including: (a) invasion of privacy; (b) financial "out of pocket" costs incurred mitigating the materialized risk and imminent threat of identity theft; (c) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (d) financial "out of pocket" costs incurred due to actual identity theft; (e) loss of time incurred due to actual identity theft; (f) loss of time due to increased spam and targeted marketing emails; (g) the loss of benefit of the bargain (price premium damages); (h) deprivation of value of their PII; and (i) the continued risk to their PII, which remains in the possession of Defendant, and which is subject to further breaches, so long as Defendant fails to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' Sensitive Information.

Plaintiff Tammy Gutierrez's Experience

74. Plaintiff Gutierrez provided her personal information to Samsung and/or its affiliates in conjunction with product and services Plaintiff obtained.

75. As part of her involvement with Defendant, Plaintiff entrusted her PII, and other confidential information such as name, address, phone number, financial account information, and other personally identifiable information to Defendant and its affiliates with the reasonable expectation and understanding that they would at least take industry standard precautions to protect, maintain, and safeguard that information from unauthorized use or disclosure, and would timely notify her of any data security incidents related to her. Plaintiff would not have permitted her PII to be given to Samsung had she known it would not take reasonable steps to safeguard her PII.

76. On or about September 2, 2022, nearly two months after Samsung's breach began, Plaintiff Gutierrez received an email from Samsung notifying her that her PII had been improperly accessed and taken by unauthorized third parties. The

notice indicated that Plaintiff Gutierrez's PII was compromised as a result of the Data Breach.

77. As a result of the Data Breach, Plaintiff Gutierrez has or will make reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching the Data Breach, reviewing credit reports, financial account statements, and/or personal records for any indications of actual or attempted identity theft or fraud.

78. Plaintiff spent this time at Defendant's direction. Indeed, in the Security Response Webpage Plaintiff was directed to, Defendant recommended Plaintiff and Class Members to:

- Remain cautious of any unsolicited communications that ask for your personal information or refer you to a web page asking for personal information
- Avoid clicking on links or downloading attachments from suspicious emails
- Review your accounts for suspicious activity.[13]

79. Plaintiff Gutierrez suffered actual injury from having her PII compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PII, a form of property that Samsung obtained from Plaintiff Gutierrez; (b) violation of her privacy rights; (c) the theft of her PII; and (d) imminent and impending injury arising from the increased risk of identity theft and fraud.

80. As a result of the Data Breach, Plaintiff Gutierrez is very concerned about identity theft and fraud, as well as the consequences of such identity theft and fraud resulting from the Data Breach.

81. The Data Breach has caused Plaintiff Gutierrez to suffer significant fear, anxiety, and stress, which has been compounded by the fact that her name and contact information and other intimate details are in the hands of criminals.

[13] https://www.samsung.com/us/support/securityresponsecenter/ (last accessed Sept. 6, 2022)

82. As a result of the Data Breach, Plaintiff Gutierrez anticipates spending considerable time and/or money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. In addition, Plaintiff Gutierrez will continue to be at present, imminent, and continued increased risk of identity theft and fraud for years to come. In fact, Plaintiff Gutierrez has received an increased number of spam calls, texts and emails.

83. Plaintiff Gutierrez has a continuing interest in ensuring that her PII, which, upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

CLASS ALLEGATIONS

84. Plaintiff brings this class action on behalf of herself and on behalf of all others similarly situated.

85. The Nationwide Class that Plaintiff seeks to represent is defined as follows:

> **All persons residing in the United States whose PII was compromised in the 2022 data breach announced by Samsung Electronics America, Inc. in September 2022. (the "Nationwide Class").**

86. The California Class that Plaintiff seeks to represent is defined as follows:

> **All persons residing in the state of California whose PII was compromised in the 2022 data breach announced by Samsung Electronics America, Inc. in September 2022. (the "California Class").**

87. Excluded from the Classes are the following individuals and/or entities: Samsung Electronics America, Inc., and Samsung's parents, subsidiaries, affiliates, officers and directors, and any entity in which Samsung has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any

aspect of this litigation, as well as their immediate family members.

88. Plaintiff reserves the right to modify or amend the definition of the proposed class and any future subclass before the Court determines whether certification is appropriate.

89. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous that joinder of all members is impracticable. Upon information and belief, there are thousands, if not millions, of individuals whose Private Information may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

90. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Class exists and predominates over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect Plaintiff's and Class Members' PII;
b. Whether Defendant had duties not to disclose the Plaintiff's and Class Members' PII to unauthorized third parties;
c. Whether Defendant had duties not to use Plaintiff's and Class Members' PII for non-business purposes;
d. Whether Defendant failed to adequately safeguard Plaintiff's and Class Members' PII;
e. Whether and when Defendant actually learned of the Data Breach;
f. Whether Defendant adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
g. Whether Defendant violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;
h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' PII;

k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

91. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of those of other Class Members because all had their Private Information compromised as a result of the Data Breach, due to Defendant's misfeasance.

92. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

93. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent and protect the interests of the Class Members in that Plaintiff has no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages Plaintiff

has suffered are typical of other Class Members. Plaintiff has also retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

94. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

95. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since they would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

/ / /

96. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

97. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

98. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure and unlawful disclosure of the Private Information of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Complaint.

99. Further, Defendant has acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

100. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

b. Whether Defendant breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their Private Information;

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

/ / /

d. Whether a contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that contract;

e. Whether Defendant breached the contract;

f. Whether an implied contract existed between Defendant on the one hand, and Plaintiff and Class Members on the other, and the terms of that implied contract;

g. Whether Defendant breached the implied contract;

h. Whether Defendant adequately and accurately informed Plaintiff and Class Members that their Private Information had been compromised;

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

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard Plaintiff's and Class Members' Private Information;

k. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I

Negligence

(On Behalf of Plaintiff and the Nationwide Class)

101. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

102. As a condition of using Defendant's products and services, Plaintiff and Class Members, as current and former users, are obligated to provide Samsung and/or its affiliates with certain PII, including but not limited to, their name, date of birth, address, contact information, and other PII depending on the product and service.

103. Plaintiff and Class Members entrusted their PII to Samsung and its affiliates on the premise and with the understanding that Samsung would safeguard

their information, use their PII for legitimate business purposes only, and/or not disclose their PII to unauthorized third parties.

104. Samsung has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

105. Samsung knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and/or using of the PII involved an unreasonable risk of harm to Plaintiff and Class Members, even if the harm occurred through the criminal acts of a third party.

106. Samsung had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Samsung's security protocols to ensure that Plaintiff's and Class Members' information in Samsung's possession was adequately secured and protected.

107. Samsung also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiff's and Class Members' PII.

108. A breach of security, unauthorized access, and resulting injury to Plaintiff and Class Members was reasonably foreseeable, particularly in light of Samsung's business as one of the largest technology company and its previous experience as the target of a cyberattack, for which the diligent protection of PII is a continuous forefront issue.

109. Plaintiff and Class Members were the foreseeable and probable victims of Samsung's inadequate security practices and procedures. Samsung knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Samsung's systems.

/ / /

110. Samsung's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Samsung's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Samsung's misconduct also included its decisions not to comply with industry standards for the safekeeping of Plaintiff's and Class Members' PII, including basic encryption techniques freely available to Samsung.

111. Plaintiff and Class Members had no ability to protect their PII that was in, and possibly remains in, Samsung's possession.

112. Samsung was in a position to protect against the harm suffered by Plaintiff and Class Members as a result of the Data Breach.

113. Samsung had and continues to have a duty to adequately and promptly disclose that Plaintiff's and Class Members' PII within Samsung's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiff and Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

114. Samsung had a duty to employ proper procedures to prevent the unauthorized dissemination of Plaintiff's and Class Members' PII.

115. Samsung has admitted that the PII of Plaintiff and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

116. Samsung, through its actions and/or omissions, unlawfully breached its duties to Plaintiff and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding Plaintiff's and Class Members' PII during the time the PII was within Samsung's possession or control.

117. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1,

PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

118. These foregoing frameworks are existing and applicable industry standards in the technology industry, and Defendant failed to comply with these accepted standards thereby opening the door to the cyber incident and causing the data breach.

119. Samsung improperly and inadequately safeguarded Plaintiff's and Class Members' PII in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

120. Samsung failed to heed industry warnings and alerts to provide adequate safeguards to protect borrower PII in the face of increased risk of theft.

121. Samsung, through its actions and/or omissions, unlawfully breached its duty to Plaintiff and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

122. Samsung, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiff and Class Members the existence and scope of the Data Breach.

123. But for Samsung's wrongful and negligent breach of duties owed to Plaintiff and Class Members, Plaintiff's and Class Members' PII would not have been compromised.

124. There is a close causal connection between Samsung's failure to implement security measures to protect Plaintiff's and Class Members' PII and the harm suffered or risk of imminent harm suffered by Plaintiff and Class. Plaintiff's and Class Members' PII was lost and accessed as the proximate result of Samsung's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

/ / /

125. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Samsung, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Samsung's duty in this regard.

126. Samsung violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Samsung's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and Class Members.

127. Samsung's violation of Section 5 of the FTC Act constitutes negligence *per se*.

128. Plaintiff and Class members are within the class of persons that the FTC Act was intended to protect.

129. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and Class.

130. As a direct and proximate result of Samsung's negligence and negligence *per se*, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest,

and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Samsung's possession and is subject to further unauthorized disclosures so long as Samsung fails to undertake appropriate and adequate measures to protect the PII in their continued possession; (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (ix) the diminished value of Samsung's goods and services they received.

131. As a direct and proximate result of Samsung's negligence, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

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

COUNT II

Unjust Enrichment

(On Behalf of Plaintiff and the Nationwide Class)

133. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

134. Plaintiff and Class Members conferred a monetary benefit on Defendant and its affiliate in the form of monetary payments—directly or indirectly—for providing products and services to current and former users.

135. Defendant collected, maintained, and stored the PII of Plaintiff and Class Members and, as such, Defendant had knowledge of the monetary benefits it

received on behalf of the Plaintiff and Class Members.

136. The money that borrowers paid to Defendant should have been used to pay, at least in part, for the administrative costs and implementation of data security adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII.

137. Defendant failed to implement—or adequately implement—those data security practices, procedures, and programs to secure sensitive PII, as evidenced by the Data Breach.

138. As a result of Defendant's failure to implement data security practices, procedures, and programs to secure sensitive PII, Plaintiff and Class Members suffered actual damages in an amount of the savings and costs Defendant reasonably and contractually should have expended on data security measures to secure Plaintiff's PII.

139. Under principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members because Defendant failed to implement the data security measures adequate to safeguard and protect the confidentiality of Plaintiff's and Class Members' PII and that the borrowers paid for.

140. As a direct and proximate result of Defendant's decision to profit rather than provide adequate security, and Defendant's resultant disclosures of Plaintiff's and Class Members' PII, Plaintiff and Class Members suffered and continue to suffer considerable injuries in the forms of time and expenses mitigating harms, diminished value of PII, loss of privacy, and a present increased risk of harm.

/ / /

/ / /

/ / /

/ / /

/ / /

COUNT III

Breach of Express Contract

(On Behalf of Plaintiff and the Nationwide Class)

141. Plaintiff restates and realleges all of the foregoing paragraphs as if fully set forth herein.

142. This count is plead in the alternative to Count II (Unjust Enrichment) above.

143. Plaintiff and Class Members allege that they were the express, foreseeable, and intended beneficiaries of valid and enforceable express contracts between Defendant and its former and current customers, contract(s) that (upon information and belief) include obligations to keep sensitive PII private and secure.

144. Upon information and belief, these contracts included promises made by Defendant that expressed and/or manifested intent that the contracts were made to primarily and directly benefit the Plaintiff and the Class (all customers entering into the contracts), as Defendant's business is for products and services for Plaintiff and the Class, but also safeguarding the PII entrusted to Defendant in the process of providing these products and services.

145. Upon information and belief, Defendant's representations required Defendant to implement the necessary security measures to protect Plaintiff's and Class Members' PII.

146. Defendant materially breached its contractual obligation to protect the PII of Plaintiff and Class Members when the information was accessed and exfiltrated by unauthorized personnel as part of the Data Breach.

147. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

148. As a direct and proximate result of the Data Breach, Plaintiff and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure of their PII,

the loss of control of their PII, the present risk of suffering additional damages, and out-of-pocket expenses.

149. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV

Breach of Implied Contract

(On Behalf of Plaintiff and the Nationwide Class)

150. Plaintiff re-alleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

151. This count is plead in the alternative to Count II (Unjust Enrichment) above.

152. Plaintiff's and Class Members' PII was provided to Defendant as part the products and services that Defendant provided to Plaintiff and Class Members.

153. Plaintiff and Class Members agreed to pay Defendant for its products and services.

154. Defendant and the Plaintiff and Class Members entered into implied contracts for the provision of adequate data security, separate and apart from any express contracts concerning the security of Plaintiff's and Class Members' PII, whereby, Defendant was obligated to take reasonable steps to secure and safeguard Plaintiff's and Class Members' PII.

155. Defendant had an implied duty of good faith to ensure that the PII of Plaintiff and Class Members in its possession was only used in accordance with its contractual obligations.

156. Defendant was therefore required to act fairly, reasonably, and in good faith in carrying out its contractual obligations to protect the confidentiality of Plaintiff's and Class Members' PII and to comply with industry standards and applicable laws and regulations for the security of this information.

/ / /

157. Under these implied contracts for data security, Defendant was further obligated to provide Plaintiff and all Class Members, with prompt and sufficient notice of any and all unauthorized access and/or theft of their PII.

158. Defendant breached the implied contracts by failing to take adequate measures to protect the confidentiality of Plaintiff's and Class Members' PII, resulting in the Data Breach.

159. Defendant further breached the implied contract by providing untimely notification to Plaintiff and Class Members who may already be victims of identity fraud or theft or are at present risk of becoming victims of identity theft or fraud.

160. The Data Breach was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

161. As a result of Defendant's conduct, Plaintiff and Class Members did not receive the full benefit of the bargain.

162. Had Defendant disclosed that its data security was inadequate, neither the Plaintiff or Class Members, nor any reasonable person would have entered into such contracts with Defendant.

163. As a result of Data Breach, Plaintiff and Class Members suffered actual damages resulting from the theft of their PII, as well as the loss of control of their PII, and remain at present risk of suffering additional damages.

164. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach, including the loss of the benefit of the bargain.

165. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

/ / /

COUNT V

Invasion of Privacy

(On Behalf of Plaintiff and the Nationwide Class)

166. Plaintiff incorporates by reference all other allegations in the Complaint as if fully set forth herein.

167. Plaintiff and Class Members have a legally protected privacy interest in their PII, which is and was collected, stored, and maintained by Defendant, and they are entitled to the reasonable and adequate protection of their PII against foreseeable unauthorized access and publication of their PII to criminal actors, as occurred with the Data Breach. The PII of Plaintiff and Class Members contain intimate details of a highly personal nature, individually and in the aggregate.

168. Plaintiff and Class Members reasonably expected that Defendant would protect and secure their PII from unauthorized parties and that their PII would not be accessed, exfiltrated, and disclosed to any unauthorized parties or for any improper purpose.

169. Defendant intentionally intruded into Plaintiff's and Class Members' seclusion by disclosing without permission their PII to a third party.

170. By failing to keep Plaintiff's and Class Members' PII secure, and disclosing PII to unauthorized parties for unauthorized use, Defendant unlawfully invaded Plaintiff's and Class Members' privacy right to seclusion by, inter alia:

a. intruding into their private affairs in a manner that would be highly offensive to a reasonable person;

b. invading their privacy by improperly using their PII obtained for a specific purpose for another purpose, or disclosing it to unauthorized persons;

c. failing to adequately secure their PII from disclosure to unauthorized persons; and

d. enabling the disclosure of their PII without consent.

171. This invasion of privacy resulted from Defendant's intentional failure to

properly secure and maintain Plaintiff's and Class Members' PII, leading to the foreseeable unauthorized access, exfiltration, and disclosure of this unguarded data.

172. Plaintiff and Class Members' PII is the type of sensitive, personal information that one normally expects will be protected from exposure by the very entity charged with safeguarding it. Further, the public has no legitimate concern in Plaintiff's, and Class Members' PII, and such information is otherwise protected from exposure to the public by various statutes, regulations and other laws.

173. The disclosure of Plaintiff's and Class Members' PII to unauthorized parties is substantial and unreasonable enough to be legally cognizable and is highly offensive to a reasonable person.

174. Defendant's willful and reckless conduct that permitted unauthorized access, exfiltration and disclosure of Plaintiff's and Class Members' intimate and sensitive PII is such that it would cause serious mental injury, shame or humiliation to people of ordinary sensibilities.

175. The unauthorized access, exfiltration, and disclosure of Plaintiff's and Class Members' PII was without their consent, and in violation of various statutes, regulations and other laws.

176. As a direct and proximate result of Defendant's intrusion upon seclusion, Plaintiff and Class Members suffered injury and sustained actual losses and damages as alleged herein. Plaintiff and Class Members alternatively seek an award of nominal damages.

COUNT VI

Violation Of the California Consumer Privacy Act, Cal. Civ. Code § 1798.150

(By Plaintiff and the members of the California Class Against Defendant)

177. Plaintiff repeat and reallege the allegations set forth in the preceding paragraphs.

178. Defendant is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues over $200 billion.

179. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140.

180. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff's and Class members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

181. Defendant collects consumers' personal information as defined in Cal. Civ. Code § 1798.140. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect this personal information. As identified herein, Defendant failed to do so.

182. As a direct and proximate result of Defendant's acts, Plaintiff's and California Class members' personal information, including phone numbers, names, date of birth, addresses, email addresses, and precise geolocation data, among other information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

183. Plaintiff and California Class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguard customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including Plaintiff's and California Class members' PII. These individuals have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information, as evidenced by its multiple data breaches.

184. On September 6, 2022, Plaintiff's counsel sent a notice letter to Samsung's corporate headquarters in New Jersey via USPS certified mail. Assuming Samsung cannot cure the Data Breach within 30 days, and Plaintiff believes such cure is not possible under these facts and circumstances, then Plaintiff intends to

promptly amend this complaint to seek actual damages and statutory damages of $750 per customer record subject to the Data Breach on behalf of the California Class as permitted by the CCPA.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of herself and all Class Members, requests judgment against Samsung Electronics America, Inc. and that the Court grant the following:

A. For an Order certifying the Nationwide Class and California Class, and appointing Plaintiff and her Counsel to represent the certified Classes;

B. For equitable relief enjoining Samsung from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class Members' PII, and from refusing to issue prompt, complete, any accurate disclosures to the Plaintiff and Class;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and the Class, including but not limited to an order:

i. prohibiting Samsung from engaging in the wrongful and unlawful acts described herein;

ii. requiring Samsung to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iii. requiring Samsung to delete, destroy, and purge the personal identifying information of Plaintiff and Class unless Samsung can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and the Class;

/ / /

iv. requiring Samsung to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiff's and Class Members' personal identifying information;

v. prohibiting Samsung from maintaining Plaintiff's and Class Members' personal identifying information on a cloud-based database;

vi. requiring Samung to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Samsung's systems on a periodic basis, and ordering Samsung to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Samsung to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Samsung to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Samsung to segment data by, among other things, creating firewalls and access controls so that if one area of Samsung's network is compromised, hackers cannot gain access to other portions of Samsung's systems;

x. requiring Samsung to conduct regular database scanning and securing checks;

xi. requiring Samsung to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Samsung to conduct internal training and education routinely and continually, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Samsung to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Samsung's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Samsung to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Samsung's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Samsung to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Samsung to implement logging and monitoring programs sufficient to track traffic to and from Samsung's servers; and

xvii. for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Samsung's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; and

/ / /

/ / /

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of punitive damages;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

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

I.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Date: October 4, 2022
Respectfully Submitted,

By, /s/ Kiley L. Grombacher

BRADLEY/GROMBACHER LLP
Marcus J. Bradley, Esq.
Kiley L. Grombacher, Esq.
Lirit A. King, Esq.

AYLSTOCK, WITKIN, KREIS & OVERHOLTZ, PLLC
Bryan F. Aylstock (*pro hac vice* pending)

Attorneys for Plaintiff and the Proposed Classes

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

TAMMY GUTIERREZ, an individual, and on behalf of classes of similarly situated individuals,

(b) County of Residence of First Listed Plaintiff Bakersfield
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*

BRADLEY/GROMBACHER, LLP; 31365 Oak Crest Drive, Suite 240 Westlake Village, CA 91361; 805-270-7100.

DEFENDANTS

SAMSUNG ELECTRONICS AMERICA, INC.

County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*

(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☒ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent—Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District *(specify)*
- ☐ 6 Multidistrict Litigation–Transfer
- ☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332

Brief description of cause:
Class Action Fairness Act ("CAFA"); privacy state-law based claim

VII. REQUESTED IN COMPLAINT:

✓ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*

JUDGE Jacqueline Scott Corley DOCKET NUMBER 3:22-cv-05176

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☒ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 10/04/2022 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Kiley L. Grombacher

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked**.** (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.