UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

LIAM MURRAY, on behalf of himself and all others similarly situated, Plaintiff, vs. SAMSUNG ELECTRONICS AMERICA, INC., Defendant.	Case No.: 1:23-cv-295 **CLASS ACTION COMPLAINT** DEMAND FOR JURY TRIAL

Plaintiff Liam Murray ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this Class Action Complaint against Samsung Electronics America, Inc. ("Samsung" or the "Defendant"), and alleges, upon personal knowledge as to his own actions and his counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiff brings this class action against Defendant for its failure to properly secure and safeguard personally identifiable information ("PII") that Defendant collected, stored, and maintained on behalf of Plaintiff and Class Members.[1] Defendant failed to comply with industry standards to protect information systems containing that PII, and for failing to provide timely, accurate, and adequate notice to Plaintiff and other Class Members that their PII had

[1] Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. 2 CFR § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual. PII also is generally defined to include certain identifiers that do not on their face name an individual, but that are particularly sensitive and/or valuable if in the wrong hands (for example, Social Security number, passport number, driver's license number, financial account number, or cellular phone location and usage data).

been accessed by an unauthorized third party and even precisely what types of information was unencrypted and accessed by unknown third parties. Plaintiff seeks, among other things, orders requiring Defendant to:

a) fully and accurately disclose the nature of the information that has been compromised:

b) adopt reasonably sufficient security practices and safeguards to prevent similar incidents in the future,

c) destroy information no longer necessary to retain for the purposes that the information was first obtained from Class Members, and

d) to provide a sum of money sufficient to provide to Plaintiff and Class Members identity theft protective services for their respective lifetimes.

2. Samsung is among the largest technology companies in the world with over $200 billion in sales and an estimated market value of over $510 billion.[2] It has millions of customers and is a leading producer of electronic goods and services including mobile phones, smartphones, televisions, and semiconductors.

3. On or around August 4, 2022, a group of cybercriminals had access to certain files on Defendant's computer network and servers containing personal information belonging to the Class Members (the "Data Breach").

4. Plaintiff and Class Members were not notified of the Data Breach until September 2, 2022, almost two months after their information was first accessed.

5. Almost two months after the actual Data Breach, Defendant posted a webpage titled "Important Notice Regarding Customer Information" (the "FAQ") to answer consumer questions

[2] Jonathon Ponciano, *The World's Largest Tech Companies - 2021,* FORBES (April 13, 2021) https://www.forbes.com/sites/jonathanponciano/2021/05/13/worlds-largest-tech-companies-2021/?sh=421d92f069bc (last visited Jan.12, 2023).

about the Breach.[3]

6. According to the FAQ, Defendant "engaged a leading outside cybersecurity firm" to review the data (stored on Defendant's systems) that was accessed in the Data Breach and confirmed that the data contained PII.

7. Defendant denied that the Breach contained consumers' "Social Security numbers or credit and debit card numbers."

8. Tellingly, Defendant stated however, that it was not sure of what was accessed at that time. Instead, Defendant stated that the Breach "may have affected information such as name, contact and demographic information, date of birth, and product registration information. The information affected for each relevant customer may vary."[4]

9. Defendant conditioned the use of certain features of Samsung products on the provision of PII by Plaintiff and Class Members. Defendant admits that it retains this information on its systems.

10. Defendant's effort to notify potential affected consumers was inadequate and marked by delay. A Computer Network and Security executive was quoted as saying: "[t]he lack of transparency on the number of individuals impacted as well as the delay in notifying them combined with a late Friday holiday weekend release seem like clear attempts to minimize the incident."[5]

11. Defendant's unexplained delay in notice to affected consumers, its lack of specificity, and its choice of timing (release of notice on "a late Friday holiday weekend") appears calculated to minimize the utility of any mitigating disclosures by Defendant.[6]

---

[3] Samsung, "Important Notice Regarding Customer Information", *available at* https://www.samsung.com/us/support/securityresponsecenter/ (last visited Jan. 12, 2023).
[4] *See Id.*
[5] Allen Bernard, *Impact of Samsung's Most Recent Data Breach Unknown*, TECHREPUBLIC (Sept. 9, 2022) http://www.techrepublic.com/article/samsung-data-breach/ (last visited Jan. 12, 2023).
[6] *Id.*

12. In fact, Defendant's nebulous description of who may be affected led a seasoned tech journalist to write: "The company did not specify which type of customers — business or consumer, for example — were impacted, give a breakdown of affected regions or provide any other information. **This lack of specificity should lead all customers to conclude that their data is part of the breach**." (Emphasis added)[7]

13. As a result of the Data Breach, Plaintiff and likely millions of Class Members suffered ascertainable losses in the form of the loss of the benefit of their bargain, out-of-pocket expenses, and the value of their time reasonably incurred to remedy or mitigate the effects of the attack and the substantial and ongoing risk of identity theft.

14. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiff's and Class Members' PII from unauthorized disclosure.

15. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their PII.

16. Plaintiff has switched to using the Linux operating system to add security to his computer files, has used a VPN to protect information over the internet, and takes great care to secure his PII.

17. Plaintiff and Class Members face a lifetime risk of identity theft, which is heightened here by the sensitivity of the data accessed and/or acquired by the cybercriminals. Plaintiff and Class Members are currently suffering, and for the rest of their lifetimes will suffer, the significant and concrete risk that their identities will be (or already have been) misused.

18. This PII was subject to unauthorized access and/or acquisition due to Defendant's

[7] Bernard, *Impact of Samsung's Data Breach Unknown, supra.*

negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiff and Class Members.

19. Plaintiff brings this action on behalf of all persons whose PII was accessed, acquired, and/or misappropriated because of Defendant's failure to: (i) adequately protect the PII of Plaintiff and Class Members; (ii) warn Plaintiff and Class Members of its inadequate information security practices; and (iii) avoid sharing the PII of Plaintiff and Class Members without adequate safeguards. Defendant's conduct amounts to negligence and violates federal and state statutes.

20. Additionally, as a result of Defendant's failure to follow contractually agreed upon, federally prescribed, industry standard security procedures, Plaintiff and Class Members received only a diminished value of the services Defendant was to provide.

21. Plaintiff and Class Members have suffered injury because of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

22. Defendant disregarded the rights of Plaintiff and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Plaintiff's and Class Members' PII was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable,

required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use.

23. Defendant has a duty to safeguard and protect customer information entrusted to it and could have prevented this theft had it limited the customer information received from its business associates, and employed reasonable measures to ensure its systems were secure from threats like ransomware attacks.

24. As the result, the PII of Plaintiff and Class Members was accessed and/or acquired by an unknown and unauthorized third party. Plaintiff and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

25. Plaintiff Liam Murray was honorably discharged from the United States Marine Corps earlier this month. He is enrolled in a New York City university and is currently residing within New York County. Plaintiff was a Samsung customer and was notified by Samsung that his PII was compromised in the Samsung data breach.

26. Defendant Samsung Electronics America, Inc. is a United States based subsidiary of Samsung Electronics Co., LTD. Defendant is incorporated in New York and headquartered at 85 Challenger Road, Ridgefield, New Jersey 07660-2118.

27. Defendant Samsung is responsible for the production and sale of billions of dollars of electronics and related services sold in the United States. Defendant Samsung does substantial business in New York and sells electronic goods and services to New York consumers.

28. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this complaint to

reflect the true names and capacities of such other responsible parties when their identities become known.

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

III. JURISDICTION AND VENUE

30. This Court has original jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2). The amount in controversy in this action exceeds $5,000,000, exclusive of interest and costs, and there are more than 100 members of the Class, defined below, many of which are citizens of a different state than Defendant. Defendant is a citizen of New Jersey, where it maintains its principal place of business. This Court has supplemental jurisdiction over any state law claims pursuant to 28 U.S.C. Section 1367.

31. This Court has personal jurisdiction over Defendant because Defendant is found within this District and conducts substantial business in this District.

32. Venue is proper in this Court under 28 U.S.C. § 1391 because Defendant is incorporated in New York state and Defendant regularly transacts business in this District with consumers of New York state living in this district, and a substantial part of the events giving rise to this Complaint arose in this District.

IV. FACTUAL ALLEGATIONS

Background

33. Samsung is a giant in the field of electronics and technology. With millions of customers, it has an estimated revenues in excess of $200 billion each year.[11]

34. Samsung manufactures a wide range of consumer and industrial electronic products

[11] Samsung, https://www.samsung.com/global/ir/financial-information/financial-valuation-snapshot/ (last visited Jan. 12, 2023).

such as televisions and home appliances (air conditioners, washer and dryers, stoves, refrigerators, and microwave ovens, etc.). Samsung's televisions and home appliances connect to the Internet and require customers to create a "Samsung Account" prior to accessing many of their devices' features.

35. Samsung also produces smart phones, smart watches, and tablets, and offers applications ("apps") for those devices. Samsung's apps include, but are not limited to, Samsung Health, Samsung Cloud, and Samsung Pay. To access the features of these devices and apps, Samsung requires customers to create a Samsung Account.

36. A "Samsung Account" is the "gateway to the World of Samsung." A Samsung Account allows customers to not only access certain features that improve the usability of the device, but a Samsung Account also provides device-related benefits that only customers with a Samsung Account can access. Those benefits include, but are not limited to, backing up and syncing data, finding a device when it is lost, device support, coupons and discounts, and order tracking.

37. Plaintiff and other proposed Class Members were required, as current and prospective customers of Samsung, to provide Samsung with sensitive PII to purchase, use, or receive Samsung's devices and services.

38. When a customer purchases a Samsung product, creates a Samsung Account, or registers for or uses a Samsung service, the customer may provide Samsung with PII such as:

- name.
- email address.
- postal address.
- phone number.
- payment card information (including name, card number, expiration date, and security code).
- date of birth.
- gender.

- information stored in or associated with the customer's Samsung Account, including the customer's Samsung Account profile, ID, username, and password.
- username and password for participating third-party devices, apps, features, or services.
- information a customer stores on a Samsung device, such as photos, contacts, text logs, touch interactions, settings, and calendar information.
- recordings of a customer's voice when they use voice commands to control a service or contact Samsung's Customer Service team; and
- location data, including (1) the precise geolocation of a customer's device if they consent to the collection of this data and (2) information about nearby Wi-Fi access points and cell towers that may be transmitted to Samsung when the customer uses certain Services.[12]

39. Samsung also collects information automatically from its customers concerning their Samsung devices such as their mobile network operator; connections to other devices; app usage information; device settings; web sites visited; search terms used; the apps, services, or features a customer downloads or purchases; and how and when those services are used.

40. Samsung, in its Privacy Policy, tells customers that:

> Our Services collect some data automatically when you use the Services. We may obtain information by automated means such as through browser cookies, pixels, web server logs, web beacons, and other technologies. Among other purposes, these technologies help us (1) remember your information so you will not have to re-enter it, (2) track and understand how you use and interact with the Services, (3) tailor the Services around your preferences, (4) manage and measure the usability of the Services, (5) understand the effectiveness of our communications, and (6) otherwise enhance the Services.[13]

41. Samsung's Privacy Policy further informs customers, including Plaintiff and Class Members, that such automatically collected information may include information about:

- your device, including MAC address, IP address, log information, device model, hardware model, IMEI number, serial number,

[12] Samsung, SAMSUNG PRIVACY POLICY FOR THE U.S., *available at* https://www.samsung.com/us/account/privacy-policy/ (last visited Dec. 20, 2022).
[13] *Id.*

> subscription information, device settings, connections to other devices, mobile network operator, web browser characteristics, app usage information, sales code, access code, current software version, MNC, subscription information, and randomized, non-persistent and resettable device identifiers, such as Personalized Service ID (or PSID), and advertising IDs, including Google Ad ID;
>
> - your use of the Services, including clickstream data, your interactions with the Services (such as the web pages you visit, search terms, and the apps, services and features you use, download, or purchase), the pages that lead or refer you to the Services, how you use the Services, and dates and times of use of the Services; and
>
> - your use of third-party websites, apps and features that are connected to certain Services.[14]

42. As a condition of providing services to its customers, Defendant collected and stored some of Plaintiff's and Class Members' most sensitive and confidential person information, including, without limitation, names, addresses and other contact information, birth dates, demographic information, and product registration information. This includes information that is static, does not frequently change, and can be used to commit myriad financial crimes.

43. Indeed, the exposure of Plaintiff's and Class Members' names, dates of birth, contact and demographic information, and product registration information increases their risk exponentially for precision spear phishing attacks, engineered SIM swaps, and the threat of credit and loans being taken out in their names.

44. Plaintiff and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

45. Defendant had a duty to adopt reasonable measures to protect Plaintiff's and Class Members' PII from involuntary disclosure to third parties.

[14] SAMSUNG PRIVACY POLICY FOR THE U.S., *supra.*

Defendant's Privacy Policies

46. On its customer-facing website, Defendant has a posted Privacy Policy for the U.S., last updated October 1, 2022 (the "Privacy Policy").[15]

47. The PII that Samsung collects from its customers is valuable to Samsung. Indeed, Samsung acknowledges this information "plays a key role in elevating what we do for our community" and that it "engage[s] with [Personally Identifiable Information] to inform and enhance everything from your experience to our communication, and to create and innovate radical solutions that help you overcome barriers."

48. The Privacy Policy states that Samsung and its affiliate parent and/or subsidiary companies "know how important privacy is to [Samsung] customers." The Privacy Policy "describes the personal information [Samsung] may obtain online across all of [its] Internet-connected Samsung devices and services (from mobile phones and tablets to TVs, home appliances, online services, and more)."

49. Samsung is also aware that its customers value their own PII. Samsung acknowledges that its customers "own" their "privacy" and recognizes "the importance [customers] place on the value of [their] privacy".

50. Because PII is valuable to Samsung's customers, Samsung made multiple promises to alleviate concerns any customers may have about providing Samsung with this sensitive information. Samsung promised its customers that: its devices and services are "designed with privacy and security at top mind"; it "take[s] data security very seriously"; it is "committed" to handling its customers Personally Identifiable Information; it "maintain[s] safeguards designed to protect personal information [Samsung] obtain[s]"; "security and privacy are at the core of what [Samsung] do[es] and what [it] think[s] about every day."

[15] *Id.*

51. Defendant further promises its customers that it has "industry-leading security" and that it "prioritize[s]" protecting customers' PII through certain security measures. Defendant states that it takes "a holistic approach to security to ensure that, at all levels of the device, [it is] protecting users' security and privacy at all times."

52. Samsung is obligated—by contract, industry standards, common law, and its representations to its customers —to keep PII confidential protecting it from unauthorized disclosures. Plaintiff and Class Members reasonably expected Samsung would comply with its own representations and its legal obligations to keep such information confidential and secure from unauthorized disclosures.

The Data Breach

53. On or about September 2, 2022, Defendant posted the Website Notice.[16] It read, in part, as follows:

> At Samsung, security is a top priority. We recently discovered a cybersecurity incident that affected some customer information.
>
> In late July 2022, an unauthorized third party acquired information from some of Samsung's U.S. systems. On or around August 4, 2022, we determined through our ongoing investigation that personal information of certain customers was affected. We have taken actions to secure the affected systems and have engaged a leading outside cybersecurity firm and are coordinating with law enforcement.
>
> We want to assure our customers that the issue did not impact Social Security numbers or credit and debit card numbers, but in some cases, may have affected information such as name, contact and demographic information, date of birth, and product registration information. The information affected for each relevant customer may vary. We are notifying customers to make them aware of this matter.
>
> At Samsung, we value the trust our customers place in our products and services – trust that we have built up over many years. By

[16] Samsung, IMPORTANT NOTICE REGARDING CUSTOMER INFORMATION (Sept. 2, 2022) *available at* https://www.samsung.com/us/support/securityresponsecenter/ (last visited Jan. 5, 2023).

> working with industry-leading experts, we will further enhance the security of our systems – and our customers' personal information – and work to maintain the trust our customers have put into the Samsung brand for more than 40 years.
>
> [. . .]
>
> We regret any inconvenience this may cause our valued customers and appreciate their trust in us.[17]

54. On or around September 2, 2022, Defendant began notifying Plaintiff and Class Members of the Data Breach. The email read, in part, as follows:

> Dear Valued Customer,
>
> At Samsung, security is a top priority. We are reaching out to inform you that Samsung recently discovered a cybersecurity incident that affected some of your information.
>
> In late July 2022, an unauthorized third party acquired information from some of Samsung's U.S. systems. On or around August 4, 2022, we determined through our ongoing investigation that personal information of certain customers was affected.
>
> We have taken actions to secure the affected systems and have engaged a leading outside cybersecurity firm and are coordinating with law enforcement. We want to assure our customers that the issue did not impact Social Security numbers or credit and debit card numbers, but in some cases, may have affected information such as name, contact and demographic information, date of birth, and product registration information. The information affected for each relevant customer may vary.
>
> At Samsung, we value the trust our customers place in our products and services - trust that we have built up over many years. By working with industry - leading experts, we will further enhance the security of our systems - and your personal information - and work to maintain the trust you have put into the Samsung brand for more than 40 years.
>
> We regret any inconvenience this may cause you and appreciate your trust in us. We have set up an FAQ page on our website for additional questions and answers along with recommended

[17] *Id.*

actions.[18]

55. In response to the Data Breach, Defendant claims that it will be "working with industry - leading experts, we will further enhance the security of [its] systems" and the personal information contained therein.[19] However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

56. Some or all of Plaintiff's and Class Members' PII that Defendant allowed to be compromised may find its way onto to the dark web, where it may be bought, sold and transferred in perpetuity, causing victims of the Data Breach untold harm. Alternatively, the wrongfully accessed, acquired, and/or misappropriated PII could simply fall into the hands of companies that will use the detailed PII and/or PHI for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

57. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing their PII to be exposed.

58. Plaintiff and Class Members have been injured by the disclosure of their PII in this Data Breach.

59. The exposure of Plaintiff's and Class Members' names, dates of birth, contact and demographic information, and product registration information increases their risk exponentially for precision spear phishing attacks, engineered SIM swaps, and the threat of credit and loans being

[18] *Screenshot*, Samsung, IMGUR.COM, available at https://i.imgur.com/JHlivkR.jpg
[19] *Id*.

taken out in their names.

60. One of the most concerning aspects of the Data Breach is the fact that the hackers stole "demographic information" from Samsung. Samsung says is collects demographic information to "help deliver the best experience possible with our products and services" (or to target specific advertising to consumers).

61. Samsung's U.S. privacy policy explains this more explicitly: "Ad networks allow us to target our messaging to users considering demographic data, users' inferred interests, and browsing context. These networks can track users' online activities over time by collecting information through automated means, including using browser cookies, web beacons, pixels, device identifiers, server logs, and other similar technologies."[20]

62. While Samsung has thus far refused to reveal what specific demographic data was stolen, TechCrunch examined Samsung's policies and concluded that this data might include: "technical information about your phone or other device, how you use your device, like which apps you have installed and which websites you visit, and how you interact with ads, which are used by advertisers and data brokers to infer information about you. The data can also include your "precise geolocation data," which can be used to identify where you go and who you meet with. Samsung says it collects information about what you watch on its smart TVs, including which channels and programs you've watched."[21]

63. Samsung also says it "may obtain other behavioral and demographic data from trusted third-party data sources," which means Samsung buys data from other companies and combines it with its own stores of customer information to learn more about you - again for targeted advertising. Samsung would not say which companies or data brokers it obtains this data

[20] Privacy Policy - SAMSUNG

[21] Zach Whittaker, *Parsing Samsung's Data Breach Notice,* TECHCRUNCH (September 6, 2022) https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice/ (last visited Dec.20, 2022).

from.

64. Following Defendant's Data Breach, this information is now likely in the hands of nefarious actors who can sell and/or use this sensitive information how they please.

65. Defendant put the burden squarely on Plaintiff and Class Members to mitigate the harm caused by this Data Breach. Defendant encouraged Plaintiff and Class Members to "review accounts" and to "[r]emain cautious of any unsolicited communications" asking for further personal information.

66. Time is a compensable and valuable resource in the United States. According to the U.S. Bureau of Labor Statistics, 55.5% of U.S.-based workers are compensated on an hourly basis, while the other 44.5% are salaried.[23] The 2018 American Time Use Survey by the Bureau states American Adults have only 36-40 hours of "leisure time" outside of work per week.[24] Usually, this time can be spent at the option and choice of the consumer. However, Defendant's failure to protect has forced Plaintiff and Class Members to spend precious time self-monitoring accounts, communicating with financial institutions and government entities, and placing other prophylactic measures in place to attempt to protect themselves.

67. Indeed, Plaintiff and all Class Members are currently at a very high risk of misuse of their PII in the coming months and years, including but not limited to unauthorized credit card charges, unauthorized access to email accounts, identity theft, and other fraudulent use of their financial accounts.

68. Plaintiff and Class Members seek renumeration for the loss of valuable time spent in the redress of Defendant's failure to protect their PII.

---

[23] *Characteristics of Minimum Wage Workers*, U.S. BUREAU OF LABOR STATISTICS REPORTS REPORT 1091 (Feb. 2021) *available at* https://www.bls.gov/opub/reports/minimum-wage/2020/home.htm#:~:text=In%202020%2C%2073.3%20million%20workers,wage%20of%20%247.25%20per%20hour (last visited Dec.21, 2022).

[24] Id.

69. Plaintiff and Class Members now face years of constant surveillance of their financial, healthcare, and personal records and accounts. Plaintiff and Class Members are incurring, and will continue to incur, such damages in addition to any fraudulent use of their PII.

Samsung's Previous Cybersecurity Failures

70. This is not Samsung's first data breach in 2022. Accordingly, Samsung should have been particularly aware of the vulnerability of its security systems.

71. On March 7, 2022, Samsung announced it had suffered a data breach that exposed internal company data, including the source code related to its Galaxy smartphones, algorithms related to Samsung smartphone biometric authentication, bootloader source code to bypass some of Samsung's operating systems controls, source code for Samsung's activation servers, and full source for technology used for authorizing and authenticating Samsung accounts.

72. The company claimed the March 2022 data breach did not include the personal information of consumers or employees. However, the incident came to light after LAPSUS$, a hacking group, leaked 190GB of Samsung's data to four hundred (400) peers.

73. Following the March 2022 data breach, Samsung promised it would "implement [] measures to prevent further such incidents and will continue to serve our customers without disruption."

74. It is possible that the Data Breach that Samsung announced on September 2, 2022, could be a continuation of the March 7, 2022 data breach.

75. Indeed, Chad McDonald, CISO of Radiant Logic, an identity and access management vendor, said "Given the difficulty of completely eliminating malware once it has infiltrated a corporate network, especially one as large and complex as Samsung's, the latest

incident could well be a continuation of the March hack."[27]

76. McDonald further stated: "The fact that they sat on this for as long as they did before they did a public disclosure implies to me they were less concerned about urgency. This makes me feel like this was quite likely just a continuation of [the former breach] they just hadn't discovered yet."[28]

77. Defendant's repeated security failures demonstrate that it failed to honor their duties and promises by not, among other things: maintaining an adequate data security system to reduce the risk of data breaches and cyber-attacks; adequately protecting Plaintiff's and the Classes' PII; and failing to reasonably limit the sensitive consumer information kept, in violation of FTC recommendations.

Defendant Acquires, Collects, and Stores Plaintiff's and Class Members' PII.

78. Defendant acquired, collected, and stored Plaintiff's and Class Members' PII.

79. As a condition of its relationships with Plaintiff and Class Members, Defendant required that Plaintiff and Class Members entrust Defendant with this highly confidential PII.

80. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

81. Plaintiff and Class Members have taken 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 business purposes only, and to make only authorized disclosures of this information.

Securing PII and Preventing Breaches

[27] Bernard, *Impact of Samsung's Most Recent Date Breach is Unknown, supra* https://www.techrepublic.com/article/samsung-data-breach/
[28] Id.

82. Defendant could have prevented this Data Breach by properly securing and encrypting the PII of Plaintiff and Class Members. Alternatively, Defendant could have destroyed the data, especially years-old data from former customers.

83. Defendant's negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

84. Despite the prevalence of public announcements of data breach and data security compromises Defendant failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

85. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[29] 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."[30]

86. The ramifications of Defendant's failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

87. The PII of individuals 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,

[29] 17 C.F.R. § 248.201(b)(9) (2022)

[30] 17 C.F.R. § 248.201(b)(8)(i) (2022)

and bank details have a price range of $50 to $200.[31] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[32] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[33]

88. As a result of Defendant's failure to properly secure Plaintiff's and the Class Members' personal identifying information, Plaintiff's and the Class Members' privacy has been invaded. Moreover, all this personal information is likely for sale to criminals on the dark web, meaning that unauthorized parties have accessed and viewed Plaintiff's and the Class Members' unencrypted, non-redacted information, including as name, contact and demographic information, date of birth, and product registration information.

89. Given all the information obtained, the criminals would also be able to create numerous fake accounts and sell sensitive information, as part of their identity theft operation.

90. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because credit and debit card accounts can be closed. The information compromised here is impossible to "close" and difficult, if not impossible, to change—name, contact information, demographic information, and troves of personal information related to technology usage.

91. This data is highly valuable on both traditional commercial markets for consumer data and on the black market for the same and can be used to commit myriad financial crimes and is valuable to criminals looking to engage in extremely specific targeted fraud schemes. Such

[31] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019) *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Dec.21, 2022).

[32] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian.com (Dec. 6, 2017) *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Dec. 21, 2022).

[33] *In the Dark*, VPN Overview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last visited Dec.21, 2022).

information can lend an air of legitimacy to nefarious actors looking to "phish" for information or money from any individual.

92. Further, among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

93. The PII of Plaintiff and Class Members was taken by hackers to ultimately engage in identity theft. The fraudulent activity resulting from the Data Breach may not come to light for years.

94. There may be a lag between the time when harm occurs versus when it is discovered; when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[34]

Defendant Failed to Comply with FTC Guidelines

95. Defendant was prohibited by the Federal Trade Commission Act ("FTC Act") (15 U.S.C. § 45) from engaging in "unfair or deceptive acts or practices in or affecting commerce." The Federal Trade Commission ("FTC") has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g. FTC v. Wyndham Worldwide Corp*., 799 F.3d 236 (3d Cir. 2015).

96. The Federal Trade Commission ("FTC") has promulgated numerous guides for

[34] U.S. GEN. ACCOUNTABILITY OFFICE REPORT TO CONGRESSIONAL REQUESTERS: PERSONAL INFORMATION at 29 (June 2007), *available at:* https://www.gao.gov/products/gao-07-737 (last visited Dec.21, 2022).

businesses that 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.[35]

97. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses.[36] The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.

98. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to private 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.[37]

99. The FTC has brought enforcement actions against businesses for failing to protect customer data adequately and reasonably, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

---

[35] FEDERAL TRADE COMMISSION, START WITH SECURITY: A GUIDE FOR BUSINESS, *available at:* https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (last visited Dec.21, 2022).

[36] FEDERAL TRADE COMMISSION, PROTECTING PERSONAL INFORMATION: A GUIDE FOR BUSINESS, *available at*: https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Dec. 21, 2022).

[37] FTC, START WITH SECURITY, *supra*.

100. Defendant failed to properly implement basic data security practices. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Plaintiff and Class Members Suffered Damages

101. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers and/or dates of birth, and of the foreseeable consequences that would occur if the PII was compromised, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result.

102. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. Plaintiff and Class Members are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

103. Defendant was, or should have been, fully aware of the unique type and the significant volume of data stored on and/or shared on its system, amounting to hundreds of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

104. Defendant's notice of Data Breach was not just untimely but woefully deficient, failing to provide basic details, including but not limited to, how unauthorized parties accessed its networks, whether the information was encrypted or otherwise protected, how it learned of the Data Breach, whether the breach occurred system-wide, whether servers storing information were accessed, and how many customers were affected by the Data Breach.

105. The offered "advice" from Defendant is insufficient to protect Plaintiff and Class Members from the lifelong implications of having their most private PII accessed, acquired,

exfiltrated, and/or published on the internet.

106. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Plaintiff Liam Murray's Experience

107. Plaintiff is customer of Samsung. As a condition of receiving services and using Samsung products Plaintiff was required to provide his personal and product information, including his name, address and other contact information, birth date, demographic information, and product registration information to Defendant.

108. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes time spent on the telephone and sorting through his unsolicited emails, verifying the legitimacy of the Data Breach, exploring credit monitoring and identity theft insurance options, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

109. Additionally, Plaintiff is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source. He uses a virtual private network ["VPN"] whenever available to secure data transmitted over the Internet.

110. Plaintiff stores any documents containing his PII in a safe and secure location. Moreover, he diligently chooses unique usernames and passwords for his few online accounts.

111. Plaintiff has taken active steps to secure his computing platform by switching to the Linux operating system, which is said to be more secure to computer hackers.

112. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Plaintiff entrusted to Defendant for the purpose

of using Defendant's products and/or services, which was compromised in and as a result of the Data Breach.

113. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

114. Plaintiff has suffered injury arising from the present and continuing risk of fraud, identity theft, and misuse resulting from his PII, including sensitive demographic information from cellular phone usage, in combination with his name, being placed in the hands of unauthorized third parties and cybercriminals.

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

V. CLASS ALLEGATIONS

116. Plaintiff brings this Nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure, and other applicable law.

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

> All Nationwide residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Cybersecurity Incident that Defendant published to Plaintiff and other Class Members on or around September 2, 2022.

118. The New York Subclass that Plaintiff seeks to represent is defined as follows:

> All New York residents whose Private Information was actually or potentially accessed or acquired during the Data Breach event that is the subject of the Notice of Cybersecurity Incident that Defendant published to Plaintiff and other Class Members on or around September 2, 2022.

119. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which

Defendant 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 and staff members.

120. Plaintiff reserves the right to modify or amend the definition of the proposed class before the Court determines whether certification is appropriate.

121. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable class. A well-defined community of interest exists to warrant class wide relief because Plaintiff and Class Members were subjected to the same wrongful practices by Defendant, entitling them to the same relief.

122. **Numerosity: Federal Rule of Civil Procedure 23(a)(1)**: The Nationwide Class is so numerous that individual joinder of its members is impracticable. While the exact number of Class Members is unknown to Plaintiff at this time, Plaintiff is informed and believes that there are at least one million Class Members. Those individuals' names and addresses are available from Defendant's records, and Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods.

123. **Commonality: Fed. R. Civ. P. 23(a)(2) and (b)(3)**. Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, common questions of law and fact exist as to members of the Nationwide Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. whether and to what extent Defendant had a duty to protect the PII of Plaintiff and Class Members;

b. whether Defendant had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. whether Defendant had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

d. whether Defendant failed to adequately safeguard the PII of Plaintiff and Class Members;

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 the PII of Plaintiff and Class Members;

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

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 currently ongoing harm faced as a result of the Data Breach.

124. **Typicality: Fed. R. Civ. P. 23(a)(3):** Consistent with Rule 23(a)(3), Plaintiff is a member of the Class he seeks to represent, and his claims and injuries are typical of the claims and injuries of the other Class Members. Plaintiff's PII was in Defendant's possession at the time of the Data Breach and was compromised as a result of the Data Breach. Plaintiff's damages and injuries are akin to other Class Members and Plaintiff seek relief consistent with the relief of the Class.

125. **Adequacy: Fed. R. Civ. P. 23(a)(4):** Consistent with Rule 23(a)(4), Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class and is committed to pursuing this matter against Defendant to obtain relief for the Class. Plaintiff has no conflicts of interest with the Class. Plaintiff's Counsel are competent and experienced in litigating class actions, including extensive experience in data breach and privacy litigation. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests

126. **Predominance & Superiority: Fed. R. Civ. P. 23(b)(3):** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. Common issues in this litigation also predominate over individual issues because those issues discussed in the above paragraph on commonality are more important to the resolution of this litigation than any individual issues. The purpose of the class action mechanism is to permit litigation against wrongdoers even when damages to individual plaintiffs may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against Defendant, and thus, individual litigation to redress Defendant's wrongful

conduct would be impracticable. Individual litigation by each Class Member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

127. **Injunctive and Declaratory Relief**. Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant has acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole. Injunctive relief is necessary to uniformly protect the Class Members' data. Plaintiff seeks prospective injunctive relief as a wholly separate remedy from any monetary relief.

128. 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 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, and safeguarding their PII;

b. whether Defendant failed to take commercially reasonable steps to safeguard the PII of Plaintiff and the Class Members;

c. whether Defendant failed to adequately monitor and audit its data security systems that stored PII; and

d. whether adherence to FTC data security recommendations, industry standards, and measures recommended by data security experts would have reasonably prevented the Data Breach.

129. **Class Actions are Fiscally Responsible and Equitable:** A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them.

130. **Risk of Prosecuting Separate Actions:** This case is appropriate for certification because class action litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

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

131. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all the prior allegations contained above.

132. Plaintiff and the Nationwide Class provided and entrusted Defendant and/or the Covered Entities with certain PII, including, without limitation, first and last first and last names, dates of birth, postal addresses, precise geolocation data, email addresses, and telephone numbers.

133. Plaintiff and the Nationwide Class 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.

134. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

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

136. Defendant 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 Defendant's security protocols to ensure that the PII of Plaintiff and the Nationwide Class in Defendant's possession was adequately secured and protected.

137. Defendant also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain pursuant to contractual obligations or state and federal regulations, including that of former customers.

138. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiff and the Nationwide Class.

139. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiff and the Nationwide Class. That special relationship arose because Plaintiff and the Nationwide Class entrusted Defendant with their confidential PII, a necessary part of their relationships with Defendant.

140. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiff and the Nationwide Class.

141. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Nationwide Class was reasonably foreseeable, particularly considering Defendant's inadequate

security practices.

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

143. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class Members. Defendant'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. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and Class Members, including basic encryption techniques freely available to Defendant.

144. Plaintiff and the Nationwide Class had no ability to protect their PII that was in, and possibly remains in, Defendant's possession.

145. Defendant was in a position to protect against the harm suffered by Plaintiff and the Nationwide Class as a result of the Data Breach.

146. Defendant had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Nationwide Class within Defendant'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 the Nationwide Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

147. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiff and Class Members.

148. Defendant has admitted that the PII of Plaintiff and the Nationwide Class was wrongfully accessed by, disclosed to, and/or acquired by unauthorized third persons as a result of

the Data Breach.

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

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

151. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiff and the Nationwide Class in the face of increased risk of theft.

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

153. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove PII it was no longer required to retain pursuant to regulations.

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

155. But for Defendant's wrongful and negligent breach of duties owed to Plaintiff and Class Members, the PII of Plaintiff and the Nationwide Class would not have been compromised.

156. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiff and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiff and Class Members. The PII of Plaintiff and the Nationwide

Class was compromised as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

157. 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 Defendant, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

158. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and failing to comply with applicable industry standards, as detailed herein. Defendant'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.

159. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

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

161. 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 Members.

162. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class 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 Defendant's possession and are subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and Class Members; and (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.

163. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class 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.

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

165. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiff and the Nationwide Class)

166. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all the allegations contained prior hereto with this complaint.

167. Defendant required Plaintiff and the Nationwide Class to provide and entrust their PII, including, without limitation, first and last first and last names, dates of birth, postal addresses, precise geolocation data, email addresses, and telephone numbers.

168. Defendant solicited and invited Plaintiff and the Nationwide Class to provide their PII to Defendant, either directly or indirectly through Defendant's customers, as part of Defendant's regular business practices. Plaintiff and the Nationwide Class accepted Defendant's offers and provided their PII to Defendant.

169. As a condition of obtaining products and/or services from Defendant, Plaintiff and the Nationwide Class provided and entrusted their personal information. In so doing, Plaintiff and the Nationwide Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Nationwide Class if their data had been breached and compromised or stolen.

170. A meeting of the minds occurred when Plaintiff and the Nationwide Class agreed to, and did, provide their PII to Defendant and/or Defendant's customers, in exchange for, among other things, the protection of their PII.

171. Plaintiff and the Nationwide Class fully performed their obligations under the implied contracts with Defendant.

172. Defendant breached the implied contracts it made with Plaintiff and the Nationwide Class by failing to safeguard and protect their PII and by failing to provide timely and accurate

notice to them that personal and financial information was compromised as a result of the Data Breach.

173. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiff and the Nationwide Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

174. As a result of Defendant's breach of implied contract, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiff and Class Members)

175. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein all prior allegations contained within this complaint.

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

177. Defendant owed a duty to its customers, including Plaintiff and Class Members, to keep the PII entrusted to it and contained in its systems confidential.

178. Defendant failed to protect and allowed access to and/or released to unknown and unauthorized third parties the PII of Plaintiff and Class Members.

179. Defendant allowed unauthorized and unknown third parties to access and examine the PII of Plaintiff and Class Members, by way of Defendant's failure to protect the PII.

180. The unauthorized release to, custody of, and/or examination by unauthorized third parties of the PII of Plaintiff and the Nationwide Class is highly offensive to a reasonable person.

181. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiff and the Nationwide Class disclosed their PII to Defendant as part of Plaintiff's and Class Members' relationships with Defendant, but privately with an intention that the PII would be kept confidential and would be protected from unauthorized disclosure. Plaintiff and the Nationwide Class were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

182. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

183. Defendant acted with a knowing state of mind when it permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

184. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiff and Class Members.

185. As a proximate result of the above acts and omissions of Defendant, the PII of Plaintiff and the Nationwide Class was disclosed to third parties without authorization, causing Plaintiff and the Nationwide Class to suffer damages.

186. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Nationwide Class in that the PII maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiff and the Nationwide Class have no adequate remedy at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiff and Class Members.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiff and Class Members)

187. Plaintiff and the Nationwide Class re-allege and incorporate by reference herein the allegations contained in all preceding paragraphs.

188. At all times during Plaintiff's and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' PII that Plaintiff and the Nationwide Class provided to Defendant and/or Defendant's customers.

189. As alleged herein and above, Defendant's relationship with Plaintiff and the Nationwide Class was governed by terms and expectations that Plaintiff's and Class Members' PII would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

190. Plaintiff and the Nationwide Class provided their PII to Defendant and/or Defendant's customers with the explicit and implicit understandings that Defendant would protect and not permit the PII to be disseminated to any unauthorized third parties.

191. Plaintiff and the Nationwide Class also provided their PII to Defendant, either directly or indirectly, with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

192. Defendant voluntarily received in confidence the PII of Plaintiff and the Nationwide Class with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

193. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, the PII of Plaintiff and the Nationwide Class was disclosed to and/or misappropriated by unauthorized third parties beyond Plaintiff's and Class Members' confidence, and without their express permission.

194. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiff and the Nationwide Class have suffered damages.

195. But for Defendant's disclosure of Plaintiff's and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' PII as well as the resulting damages.

196. The injury and harm Plaintiff and the Nationwide Class suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' PII. Defendant knew or should have known its methods of accepting and securing Plaintiff's and Class Members' PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiff's and Class Members' PII.

197. As a direct and proximate result of Defendant's breach of its confidence with Plaintiff and Class Members, Plaintiff and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity 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 Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiff and Class Members; and (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.

198. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class 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.

199. As a result of Defendant's breaches of confidence, Plaintiff and the Nationwide Class are entitled to and demand actual, consequential, and nominal damages.

COUNT V
VIOLATIONS OF NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiff and New York Class Members Resident or Injured in During Class Period)

200. Plaintiff and the New York Subclass re-allege and incorporate by reference herein all the allegations contained in the preceding paragraphs.

201. Plaintiff brings this claim on behalf of himself and the New York Subclass [hereinafter "Subclass"].

202. Plaintiff and Subclass are persons within the meaning of New York General Business Law ("GBL") § 349(h).

203. GBL § 349(a) prohibits "[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state". Defendant engaged in deceptive acts and practices in the form of misrepresentations and omissions during the conduct of business in and from New York by engaging in the methods, acts, practices, and conduct described in this Complaint, including but not limited to (i) establishing the sub-standard security practices and procedures described herein; (ii) soliciting and collecting the PII of Plaintiff and Subclass with the knowledge that the information would not be adequately protected; (iii) storing Plaintiff's and Subclass member's PII in an unsecure environment and failing to take reasonable methods to safeguard said PII; (iv) making false, misleading, deceptive and/or inaccurate statements, and omitting material facts, concerning Defendant's security measures, expertise, and vigilance in the care and handling of PII within all user accounts; (v) making false, misleading, deceptive, and/or inaccurate statements, and omitting material information concerning the safety and security of the PII provided by Plaintiff and Subclass as a condition precedent to the opening and/or registration of Samsung accounts; and (vi) engaging in unlawful acts and practices by failing to disclose the Data Breach to New York Subclass members in a timely and accurate manner.

204. Defendant's failure to adequately notify Plaintiff and the New York Subclass of the precise nature of the breach, exactly who was affected by said breach, and its deliberate release of the news on a Friday of a major holiday weekend amounts to an egregious act of deception that injured Plaintiff and the New York Subclass.

205. By engaging in the above acts and practices, Defendant has committed an "unlawful act or practice" within the meaning of § 349 of the GBL. Plaintiffs and Subclass members have suffered substantial injury they could not reasonably have avoided other than by not purchasing the Defendant's products and/or services and providing the required PII to do so.

206. Defendant's violations of GBL § 349(a) have directly, foreseeably, and proximately caused damages and injury to Plaintiff and Subclass. Plaintiff and Subclass relied on, and made their purchasing decisions, wholly or in part based on Defendant's representations regarding its security measures and trusted that Defendant would keep their PII safe and secure. Accordingly, Plaintiff and Subclass provided their PII to Defendant with the reasonable belief and expectation that their PII would be safe, private, and secure and any mishap would be handled expediently, expertly, and with full disclosure of the material facts – something Defendant wholly failed to do. Instead, its notification of the breach was misleading, incomplete, and inaccurate. The Defendant resorted to obfuscation with its untimely notification released on the Friday of a major holiday weekend.

207. As a direct and proximate cause of Defendant's unlawful practices and acts, Plaintiff and Subclass residing in New York suffered injury as a result of the Defendants actions and inactions. This injury was compounded by the failure by Defendant to adequately and timely notify Plaintiff and Subclass of the breach. As such, they are entitled to pursue claims against Defendant for damages, including but not limited to (i) to the price received by Defendant's for products and services; (ii) the loss of Plaintiff's and Subclass member's legally protected interest in the confidentiality and privacy of their PII, (iii) the costs of protecting Plaintiff and Subclass from further injury by the release of their PII to the dark web, (iv) additional losses described above.

208. Defendant knew or should have known that Defendant's system of information storage and data security practices were inadequate to safeguard the vital PII provided at Defendant's behest by Plaintiff and Subclass. Defendant knew or should have known that the risk of data breach or theft was highly likely, especially given Samsung's prior breach of March 2022. Defendant's actions engaging in the above-described unlawful practices and acts were negligent

at best. At worst, they were a knowing, willful and/or wanton and reckless disregard to the rights of Plaintiff and Subclass.

209. Plaintiff and Subclass seek relief under N.Y. GBL § 349 including, but not limited to, restitution for money or other financial benefit that Defendant may have acquired by means of Defendant's unlawful acts or practices, damages and restitution for actual losses "or fifty dollars, whichever is greater" suffered as a result of said unlawful acts and practices, declaratory relief, and attorney's fees and costs. Additionally, Plaintiff and Subclass seek treble damages under section 349(h) which provides for the award of damages "to an amount not to exceed three times the actual damages up to one thousand dollars, if the court finds the defendant willfully or knowingly violated this section."

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself, Nationwide Class, and Subclass Members, requests judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class and appointing Plaintiff and their counsel to represent such Class;

B. For an Order certifying the New York State Class and appointing Plaintiff and their Counsel to represent such Class;

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

D. 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 Class Members, including but not limited to an order:

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

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

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

v. prohibiting Defendant from maintaining the PII of Plaintiff, the Nationwide Class and the New York State Subclass on a cloud-based database;

vi. requiring Defendant 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 Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

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

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

ix. requiring Defendant to segment data by, among other things, creating firewalls

and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks.

xi. requiring Defendant 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 Defendant to routinely and continually conduct internal training and education, 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 Defendant 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 employee's compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

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

xv. requiring Defendant to meaningfully educate all the Nationwide Class and New

York State Class 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 Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and 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 Defendant'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;

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

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.

DEMAND FOR JURY TRIAL

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

Date: January 12, 2023

THE LAW OFFICE OF PAUL C. WHALEN, P.C.

/s/Paul C. Whalen

_____

PAUL C. WHALEN, ESQ.
[PW1300]
768 Plandome Road
Manhasset, NY 11030
(516) 426-6870
(631) 612-3905
pcwhalen@proton.me

Attorney for Plaintiff and the Putative Class

ClassAction.org
