CLARKSON LAW FIRM, P.C.
Ryan J. Clarkson (SBN 257074)
Katherine A. Bruce (SBN 288694)
Bahar Sodaify (SBN 289730)
Yana Hart (SBN 306499)
22525 Pacific Coast Highway
Malibu, CA 90265
Tel: (213) 788-4050
Email: rclarkson@clarksonlawfirm.com
Email: kbruce@clarksonlawfirm.com
Email: bsodaify@clarksonlawfirm.com
Email: yhart@clarksonlawfirm.com

TYCKO & ZAVAREEI LLP
Sabita J. Soneji (SBN 224262)
1970 Broadway, Suite 1070
Oakland, CA 94612
Tel: (510) 250-3370
Email: ssoneji@tzlegal.com

TYCKO & ZAVAREEI LLP
Hassan A. Zavareei (SBN 181547)
1828 L Street NW, Ste. 1000
Washington, DC 20036
Tel: (202) 973-973-0900
Email: hzavareei@tzlegal.com

Counsel for Plaintiffs and the Proposed Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

NAEEM SEIRAFI and SHELBY HOLTZCLAW, individually and on behalf of all others similarly situated,

Plaintiffs,

vs.

SAMSUNG ELECTRONICS AMERICA, INC., a corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT

1. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE SECTION 17200, *et seq.*
2. VIOLATION OF CALIFORNIA CONSUMERS LEGAL REMEDIES ACT, CIVIL CODE SECTION 1750, *et seq.*
3. VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT ("CCPA"), CAL. CIV. CODE SECTION 1798.150, *et seq.*
4. DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE SECTIONS 1709, 1710
5. VIOLATION OF MICHIGAN IDENTITY THEFT PROTECTION ACT, MICH. COMP. LAWS ANN. SECTION 445.72, *et seq.*
6. VIOLATION OF MICHIGAN CONSUMER PROTECTION ACT, MICH. COMP. LAWS ANN. SECTION 445.903, *et seq.*
7. NEGLIGENCE
8. INTENTIONAL MISREPRESENTATION
9. BREACH OF EXPRESS WARRANTY
10. BREACH OF IMPLIED WARRANTY

DEMAND FOR JURY TRIAL

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Plaintiffs Naeem Seirafi ("Seirafi") and Shelby Holtzclaw ("Holtzclaw"), individually and on behalf of all others similarly situated, ("Plaintiffs") bring this Action against Defendant Samsung Electronics America, Inc. ("Samsung" or "Defendant"). Plaintiffs' allegations are based upon personal knowledge as to themselves and their own acts, and upon information and belief as to all other matters based on the investigation conducted by and through Plaintiffs' attorneys. Plaintiffs believe that substantial additional evidentiary support will exist for the allegations set forth herein, after a reasonable opportunity for discovery.

I. INTRODUCTION

1. Samsung is among the top five largest technology companies in the world, and the second largest in 2021, with over $200 billion of annual revenue and over a $360 billion market cap.[1] It is a major producer of a wide array of electronic devices, including mobile phones, smartphones, televisions, and semiconductor chips. Plaintiffs and millions of other consumers entrusted Samsung with their personal data when they registered for Samsung accounts, providing their names, dates of birth, postal addresses, precise geolocation data, email addresses, phone numbers, the Samsung products they own, and other information. As stated in their own privacy policy, Samsung recognizes the heavy burden of protection and security that they bear when collecting and storing this data.[2] Indeed, Samsung represents that it maintains "safeguards designed to protect personal information."[3] Samsung touts its purported dedication to strong security by making the following advertising claims for its devices and services, including but not limited to, the following: [4,5]

[1] *See* Kim Eun-jin, *Samsung Electronics Ranked 4th in Forbes' List of World's Largest Tech Companies,* BUSINESS KOREA (May 16, 2022, 4:48 PM), http://www.businesskorea.co.kr/news/articleView.html?idxno=92787.
[2] *See Samsung Privacy Policy for the U.S.*, SAMSUNG, https://www.samsung.com/us/account/privacy-policy/ (last updated Oct. 1, 2021).
[3] *Id.*
[4] *See Welcome to Samsung Mobile Security*, SAMSUNG MOBILE SECURITY, https://security.samsungmobile.com/main.smsb (last visited September 8, 2022).
[5] *See Why Galaxy?*, SAMSUNG, https://www.samsung.com/us/mobile/why-galaxy/#privacy (last visited September 8, 2022); *Secure. Secured by Knox.*, SAMSUNG, https://www.samsung.com/us/security/ (last visited September 8, 2022).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

"[O]ur dedicated security team continuously audits Samsung devices and services so that users can have peace in mind with Samsung's industry-leading security."[6]

"[W]e recognize the importance of protecting our users' security and privacy."[7]

"[S]ecurity and privacy are at the core of what we do and what we think about every day."[8]

2. Samsung's representations of strong and robust security have proved false and misleading—Samsung admittedly failed to safeguard the sensitive personal identifying information of millions of its consumers, or implement robust security measures to prevent this information from being stolen.

II. PARTIES

3. Plaintiff Seirafi is an individual residing in California, who had his personal identifiable information ("PII") exfiltrated and compromised in the data breach *announced* by Defendant on September 2, 2022. Seirafi purchased two Samsung printers, one online in September of 2015, and one at a BestBuy store in California in 2018. To gain access to certain features such as software drivers and the printer application for MacOS, Seirafi was required to create a Samsung account and register the devices. Seirafi created an account and registered both devices on October 2, 2018. In doing so, Seirafi was required to provide Defendant with his name, postal address, email address, date of birth, and phone number, among other information. In making his decision to create a Samsung account to gain full access to the products' features, Seirafi reasonably expected that Defendant would safeguard his PII. Seirafi would not have purchased the products, nor would he have created a Samsung account, if he knew that the sensitive information collected by Defendant would be at risk. Seirafi has suffered damages and remains at a significant risk now that his PII has been leaked online.

4. Plaintiff Holtzclaw is an individual residing in Michigan, who had her PII exfiltrated and compromised in the data breach *announced* by Defendant on September 2, 2022. Holtzclaw

[6] *Welcome to Samsung Mobile Security*, SAMSUNG MOBILE SECURITY, https://security.samsungmobile.com/main.smsb (last visited September 8, 2022).
[7] *Id.*
[8] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

purchased a Samsung Smart TV in Michigan in approximately Spring 2022. Holtzclaw was required to create a Samsung account in order to use the TV and access its features. In doing so, Holtzclaw was required to provide Defendant with her name, postal address, email address, date of birth, and phone number, among other information. In making her decision to create a Samsung account, Holtzclaw reasonably expected that Defendant would safeguard her PII. Holtzclaw would not have purchased the TV, nor would she have created a Samsung account, if she knew that the sensitive information collected by Defendant would be at risk. Holtzclaw has suffered damages and remains at a significant risk now that her PII has been leaked online.

5. Defendant Samsung Electronics America, Inc. is a United States based subsidiary of Samsung Electronics Co., Ltd., and is responsible for the production and sale of billions of dollars of electronics sold in the United States. Defendant is incorporated in New York and headquartered in New Jersey. Importantly, upon information and belief, Defendant maintains main offices and employees who specifically oversee and handle data privacy, data policies, and make data-driven decisions in San Francisco, California. In fact, Defendant's Vice President who handles "Big Data" practices for is located in San Francisco, CA.[9] Defendant's Vice President is in charge of managing one of the "largest and most dynamic" "Big Data" practices.[10] Therefore, it appears that the data-related privacy policies, protections, important decisions impacting consumers' data, and other "data driven decision making processes" stem from Defandant's San Francisco offices.

III. JURISDICTION AND VENUE

6. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section 1332 of 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. Section 1367.

[9] Saurabh Sharma, LINKEDIN, (accessed on September 9, 2022), https://www.linkedin.com/in/saurabh-sharma-9b0aa38/

[10] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

7. Pursuant to 28 U.S.C. Section 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.

8. 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.

IV. FACTUAL ALLEGATIONS

9. Defendant is a technology and electronics giant that sells millions of products and produces over $200 billion of revenue each year.[11] Defendant is worth over $45 billion, has sold over 2 billion smartphones, and employs over 250,000 people.[12] It produces a wide array of electronic devices but is best known for being a top manufacturer of mobile phones, smartphones, televisions, and semiconductor chips.

10. Defendant collects and processes the personal data of millions of consumers, including personal information obtained across all of Samsung's Internet-connected Samsung devices and services (from mobile phones and tablets to TVs, home appliances, online services, and

[11] *Samsung Revenue: Sales, Manufacturing, Employees | 2012-2022*, MIRROR MEISTER (Jan. 1, 2021), https://www.mirrormeister.com/samsung-revenue-productions-stats/.
[12] *Id.*

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

more).[13] For nearly all of its products and services, Defendant requires that consumers create a Samsung account, forcing consumers to entrust Defendant with their PII, in order to use Defendant's products and services. In fact, regardless of whether a consumer buys a printer, television, or a smartphone, consumers need to register their products with Samsung to access the features of their devices. Consumers are therefore forced to register accounts, otherwise many product features are locked/inaccessible, or even using the products in the way they were intended, is nearly impossible without this required registration.

11. Defendant also requires consumers to register the products for warranty-related registration, gaining access to the Samsung Galaxy Store (Defendant's equivalent of the App Store or Google Market), or even accessing certain drivers or software. These features are essential to the function of the devices sold by Defendant, and consumers must create an account to access the full features of their devices.

12. Many features which are advertised and promised by Defendant with the sale of products, can only be accessed *after* a consumer creates a Samsung account. By locking features, making products' software updates inaccessible, and inhibiting intended use of products, Defendant ensures that nearly every consumer who purchased any of the Defendant's devices, at some point, is required to provide their personal information through this mandatory registration in order to use the products.

13. Users who create Samsung accounts also cannot gain access to the product-related benefits that users with an account are able to access. These benefits include but are not limited to: product support, order tracking, exclusive rewards and offers, Samsung Rewards, Galaxy Store, Samsung Pay, Samsung Health, Samsung Members, and Samsung TV Plus.[14]

14. The information collected and stored by Defendant includes, but is not limited to, ***names, dates of birth, addresses, precise geolocation data, email addresses, phone numbers, and information about the products each consumer owns***. Defendant collected this PII by requiring

[13] *See supra* note 2.

[14] *See Samsung Account Benefits*, SAMSUNG, https://www.samsung.com/us/samsung-account-benefits/ (last visited September 9, 2022).

consumers to complete account registration, for consumers to gain the full use of the purchased products.

15. Defendant holds itself as a trustworthy company, which recognized and values the customers' privacy and personal information, and has repeatedly assured its customers that it "maintain[s] safeguards designed to protect personal information we obtain through the Services."[15] Further, Defendant makes representations that it has the "industry-leading security," that "security and privacy are at the core of what [they] do and what [they] think about every day," and that its "holistic approach to security" ensures that they "are protecting users' security and privacy at all times."[16]

16. Defendant's privacy policy and online advertisements clearly and unequivocally state that any personal information provided to Defendant will remain secure and protected.

17. For many years, Defendant represented and continues to represent its "commitment" to value and protecting consumer privacy:

Our approach to privacy

Whether you are using our phones, watching our TVs, paying for goods with our digital wallet, measuring your fitness with our apps, or making your home smarter, we strive to provide you a seamless experience. In order to deliver these experiences in a way that adds value to you, there are often times when Samsung needs to collect data about your usage.

At Samsung, **we recognize the importance you place on the value of your privacy and we want you to know that we do too.**

When you use Samsung products or services, you may provide information about who you are, who you call or text, what shows you watch, or what you view online. **We recognize the importance of protecting your information. Our products and services are designed with privacy and security at top of mind**. Let us tell you a bit more about how.
Galaxy Phones & Privacy: our phones have many features that help you to protect your data should your phone be used without permission, lost or stolen. Features such as fingerprint, facial and iris authentication to help ensure that you, and only you, can access and use your phone.

Knox & Privacy: **the protection of your personal data is underwritten by industry leading security. Samsung has developed a defense-grade security solution called Knox that is built into the architecture of our products.** Data that you store in Knox is shielded by one of the highest levels of encryption

[15] *Samsung Privacy Policy for the U.S.*, SAMSUNG, https://www.samsung.com/us/account/privacy-policy/ (last updated Oct. 1, 2021).
[16] *See Samsung Mobile Security*, SAMSUNG, https://security.samsungmobile.com/main.smsb/ (last accessed September 8, 2022)

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

> currently available. This technology is not just for mobile devices. It can be the key to securing information traveling through connected devices in the world of the Internet of Things (IoT).
>
> Payments & Privacy: our digital wallet, Samsung Pay, incorporates a technology called tokenization that means you don't use your actual credit card number for payment transactions, and enables you to use your phone with little worry that your account numbers will be exposed.
>
> SmartTVs & Privacy: **we've embedded encryption on our TVs for the storage and transmission of your information whenever you use apps or surf the internet.**
>
> Appliances: Connected appliances such as our Family Hub refrigerators use information you provide to enable features such as calendar sharing and shopping list. These devices also feature services that allow you to order products through third parties. the data is protected with industry standard encryption to help protect your information.
>
> These are some of the ways that **we have sought to empower you, our customer, to protect yourself and your information**. We would be remiss if we didn't also talk to you about how we use information that you choose to give to us when you enjoy our products and services.
>
> Our priority as a company is to utilize information to enhance your customer experience with our products and services. We challenge ourselves to think of you first and our innovation is driven by how people use our products. We use data to inform ourselves about what you use and like, and what you are not so crazy about. Delivering to you, our customer, a personalized, seamless experience that you find valuable can only be crafted if we know what works for you. So we provide notices to you about the types of information that are used in order to deliver that seamless experience.
>
> Innovation is continually changing and so do privacy implications that accompany it. As such, we are constantly looking for ways to improve our interaction with you by seeking to strike the right balance between protecting your privacy while providing the best possible experience. That is our enduring commitment.[17]

18. Plaintiffs and other similarly situated consumers relied to their detriment on Defendant's uniform representations and omissions regarding data security, including Defendant's failure to alert customers that its security protections were inadequate, and that Defendant would forever store Plaintiffs' and customers' PII, failing to archive it, protect it, or at the very minimum warn consumers of the anticipated and foreseeable data breach.[18]

19. Had Defendant disclosed to Plaintiffs and its other customers that its data systems were not secure at all and, were vulnerable to attack, Plaintiffs would not have purchased

[17] Samsung, *Our Approach to Privacy*, WAYBACK MACHINE, (Jan. 10, 2018), https://web.archive.org/web/20180110190948/https://www.samsung.com/us/account/our-approach-to-privacy/. (emphasis added).

[18] *Important Notice Regarding Customer Information*, SAMSUNG (Sept. 2, 2022), https://www.samsung.com/us/support/securityresponsecenter/?nrtv_cid=1fb58bb166ff46ba7092773f1d8ac8ab792dd710a900fe074c6b9f4f9df87eb0&cid=opmc-ecomm-nrtiv-pc-042720-142005-future-13050610&utm_source=future&utm_medium=narrativ&utm_campaign=13050610&utm_content=pc&nrtv_as_src=1.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Defendant's products or utilized its services. In fact, Defendant would have been forced to adopt reasonable data security measures and comply with the law.

20. Plaintiffs and other similarly situated consumers trusted Defendant with their sensitive and valuable PII. Defendant did not need to collect this PII at all. It did so, to increase its profits, gather the information regarding its customers, and be able to track their customers and their behaviors. For instance, when Plaintiff Seirafi purchased his printers – there was absolutely no need for Defendant to gather Plaintiff Seirafi's information. Plaintiff Seirafi (as many other consumers) could not have expected that purchasing a printer and registering his account (as it was required by Defendant) would lead to Defendant's misuse of Plaintiff Seirafi's PII, constant use of Plaintiff Seirafi's PII – even *years following the purchase* – failure to archive Plaintiff Seirafi's PII, failure to implement appropriate security measures, and prevent the access to Plaintiff Seirafi's PII.

21. Similarly, Plaintiff Holtzclaw, in purchasing Defendant's TV and registering her account with Defendant to access its features and use the TV, would result in Defendant's misuse of her PII, leading to this data breach.

22. Defendant knew or should have known that Plaintiffs and Class Members would reasonably rely upon and trust Defendant's promises regarding security and safety of their data and systems.

23. By collecting, using, selling, monitoring, and trafficking Plaintiffs' and other customers' PII, and utterly failing to protect it by maintaining inadequate security systems, failing to properly archive the PII, allowing access of third parties, and failing to implement security measures, Defendant caused harm to Plaintiffs and consumers.

FIRST DATA BREACH

24. At all material times, Defendant failed to maintain proper security measures despite its promises of safety and security to consumers.

25. In April 2022, an organization called Lapsus$ accessed and stole Defendant's various confidential data.[19] Lapsus$ published ***190GB of Samsung's confidential data online***.

[19] *See* Mike Moore, *Samsung Confirms Data Breach, Personal Customer Data Stolen*, TECHRADARPRO (Sept. 5, 2022), https://www.techradar.com/news/samsung-confirms-data-breach-personal-customer-data-stolen.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

26. Despite this initial data breach, Defendant continued to maintain and reassure its customers that their data was safe, and only "some source code relating to the operation of Galaxy devices" was released while the "personal information of [Defendant's] customers [and] employees" was safe.[20] Defendant minimized entirely the impact of this first data breach, failing to warn consumers, and implement the proper measures to prepare for the second attack.

27. During this first data breach, Lapsus$ claimed to have taken the sources for every Trusted Applet installed in Samsung's TrustZone environment used for sensitive operations; algorithms for all biometric unlock operations; bootloader source code for all recent Samsung devices; confidential source code from Qualcomm; ***source code for Samsung's activation servers; full source code for technology used for authorizing and authenticating Samsung accounts***, including APIs and services.[21]

28. Despite this earlier breach and full knowledge of the exposed sensitive technical data and the immediate need to protect customers' private information and data from Lapsus$ and other attackers, Defendant utterly failed to adequately secure its systems, and allowed another breach to occur, this time compromising consumer PII. Nevertheless, after this first violent threat and compromise of the data that fueled and facilitated the subsequent second data breach and access of customers' PII, Defendant falsely re-assured consumers that it does not expect its operations to be too disturbed by the incident (i.e. first data breach.)[22]

29. At the very minimum, Defendant failed to archive customers' PII, increase the layer of security for the customers' PII, prevent customers' PII to be accessible online (by moving this data to different servers, for example), and taking other actions to ensure the safety of personal data and credentials.

SECOND DATA BREACH

30. Defendant once again failed to implement any effective security measures to prevent a data breach, leading to its second, and most current, data breach. Indeed, despite Defendant's full

[20] Sead Fadilpasic, *Samsung Confirms Cyberattack, Says Internal Data Leaked*, TECHRADAR (April 14, 2022), https://www.techradar.com/news/samsung-hacked-galaxy-phones-leaked.
[21] *Id.*
[22] *Id.*

knowledge of the sensitivity of stolen data, and re-assurances to worried customers and the public that no PII was lost or accessed, and its representations that Defendant expected its operations not to be too disturbed by the "incident," Defendant failed to implement any proper security measures to prevent the second attack.

31. Defendant was aware that its systems were vulnerable to the further attack by unauthorized third parties, and more importantly, it was aware that the fraudsters and criminals who had access to the stolen source codes and authentication-related information (among other confidential data) could penetrate Defendant's weak systems. Defendant could have taken measures to prevent the next attack but failed to do so.

32. In July 2022, an undisclosed but large quantity of the PII entrusted to Defendant was exfiltrated and stolen by an "unauthorized third party."

33. Defendant claims that it did not even learn of this attack until about August 4, 2022, at which point, the fraudsters could have downloaded and accessed numerous data of Defendant's customers.

34. To date, Defendant fails to explain the scope of this breach, or notify all affected customers.

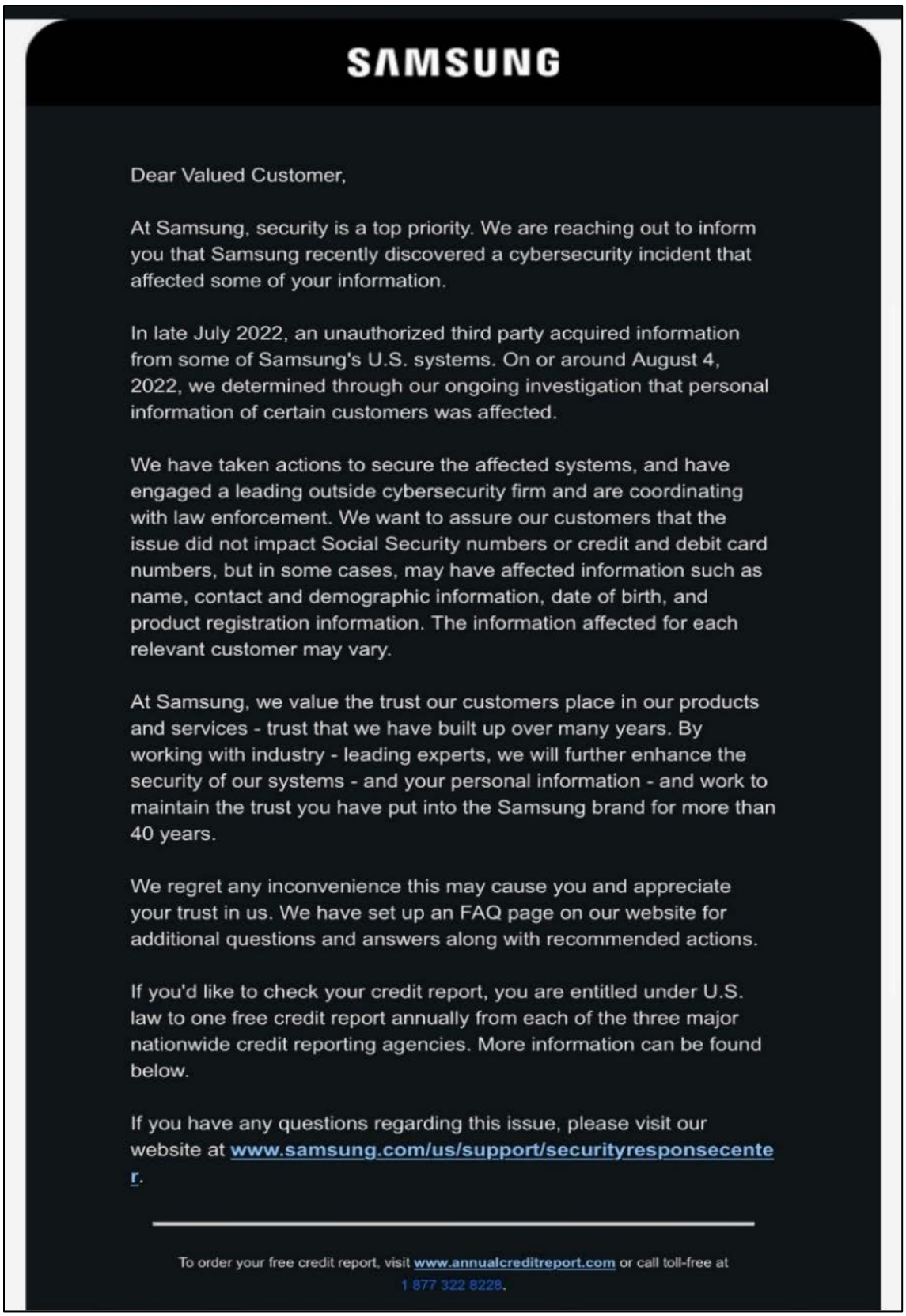
35. Defendant confirmed that this PII included "information such as name, contact and demographic information, date of birth, and product registration information."[23]

36. Nevertheless, despite **knowing** about this attack as of August 4, 2022, Defendant did not release a statement to affected consumers until September 2, 2022, ***up to two months after*** the breach happened, and ***nearly an entire month*** after they became aware that consumers' data had

[23] *Important Notice Regarding Customer Information*, SAMSUNG (Sept. 2, 2022), https://www.samsung.com/us/support/securityresponsecenter/?nrtv_cid=1fb58bb166ff46ba7092773f1d8ac8ab792dd710a900fe074c6b9f4f9df87eb0&cid=opmc-ecomm-nrtiv-pc-042720-142005-future-13050610&utm_source=future&utm_medium=narrativ&utm_campaign=13050610&utm_content=pc&nrtv_as_src=1.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

been accessed and exfiltrated. A true and correct image of the statement Samsung released to Plaintiff and other consumers is set forth below.



SAMSUNG

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 actions.

If you'd like to check your credit report, you are entitled under U.S. law to one free credit report annually from each of the three major nationwide credit reporting agencies. More information can be found below.

If you have any questions regarding this issue, please visit our website at www.samsung.com/us/support/securityresponsecenter.

To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1 877 322 8228.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

37. Both Plaintiffs received this statement regarding the breach; however, Defendant has yet to notify numerous other consumers who were affected by this breach.

38. In its statement, Defendant does not disclose how many consumers' PII was breached, leaving consumers to speculate whether it is likely that their PII has been compromised and without any clear instruction on what they can do to protect themselves now that their PII has been exposed. It is believed that *greater than half* of Samsung's US consumers had their PII compromised in the breach.[24]

39. In fact, many customers are yet to learn that their information has been misused and subject to this data breach as the result of Defendant's utter failure to implement appropriate security measures.

IMPACT OF DATA BREACH ON CONSUMERS

40. Plaintiffs and the Class have suffered actual harm as a result of Defendant's conduct. Defendant failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. This breach allowed hackers to access the PII, including first and last names, postal addresses, precise geolocation data, email addresses, and telephone numbers, for Plaintiffs and the Class. This PII has since been publicly leaked online, which has allowed for digital and potential physical attacks against Plaintiffs and the Class. Now that the PII has been leaked, it is available for other parties to sell or trade and will continue to be at risk for the indefinite future. In fact, the U.S. Government Accountability Office found that, "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."[25]

Digital Phishing Scams

41. Phishing scammers use emails and text messages to trick people into giving them their personal information, including but not limited to passwords, account numbers, and social security

[24] *See* Zack Whittaker, *Parsing Samsung's Data Breach Notice*, TECHCRUNCH (Sept. 6, 2022, 10:00 AM), https://techcrunch.com/2022/09/06/parsing-samsung-july-breach-notice/.
[25] *See* U.S. GOV'T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS 29 2007. https://www.gao.gov/new.items/d07737.pdf.

numbers. Phishing scams are frequently successful, and the FBI reported that people lost approximately $57 million to such scams in 2019 alone.[26]

42. As a result of the data breach, Plaintiffs and the Class have received a high-volume of phishing emails and spam telephone calls. Such scams trick consumers into giving account information, passwords, and other valuable personal information to scammers. This significantly increases the risk of further substantial damages to Plaintiffs and the Class, including, but not limited to, monetary and identity theft. On average, Plaintiffs have received twenty or more phishing emails since the data breach and have noticed a substantial increase in spam telephone calls. Many of the phishing emails received by Plaintiffs and the Class are disguised as coming from actual reputable companies, but are instead traps to further steal their PII. Due to the breach, Plaintiffs and the Class now need to spend a substantially increased amount of time and effort discerning between genuine emails and emails that are trying to phish their PII.

43. Plaintiffs are suffering ongoing fraud and phishing attacks from various individuals who were able to get ahold of Plaintiffs' personal data as a result of this data breach. Plaintiffs are receiving ongoing attacks by persons posing as various companies or providers, attempting to seek further personal identifying information, attempting to reset their passwords, and gain access to other accounts.

44. The data leak also caused an increased number of fraudulent calls and text messages to Plaintiffs and the Class. Plaintiffs have been receiving numerous digital attacks as a result of this data breach.

45. Plaintiffs are suffering ongoing phishing attacks from various individuals who were able to get ahold of Plaintiffs' data. Furthermore, this data appears to be shared with other fraudsters across the dark web, as Plaintiffs' ongoing attacks are increasing.

46. Given the highly sensitive nature of the information stolen, and its dissemination to unauthorized parties, Plaintiffs have already suffered injury and remain at a substantial and imminent risk of future harm.

[26] *See How to Recognize and Avoid Phishing Scams*, FTC Consumer Advice, https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams (last visited Sept. 8, 2022).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

SIM-Swap

47. The data leak can also lead to SIM-swap attacks against the Class.[9] A SIM-swap attack occurs when the scammers trick a telephone carrier to porting the victim's phone number to the scammer's SIM card. By doing so, the attacker is able to bypass two-factor authentication accounts, as are used to access cryptocurrency wallets and other important accounts. The type of personal information that has been leaked poses a profound tangible risk of SIM-swap attacks for the Class.

48. Defendant's customers are now more likely to become victims of SIM Swap attacks because of the release personal information.

Loss of Time

49. As a result of this breach, Plaintiffs suffered unauthorized email solicitations, and experienced a significant increase in suspicious phishing scam activity via email, phone calls, text messages, all following the breach. In addition, both Plaintiffs, as a result of the breach spent significant time and effort researching the breach, monitoring their accounts for fraudulent activity, reviewing the unsolicited emails, texts, and answering telephone calls.

50. Each Plaintiff also spent significant time monitoring personal accounts (banking, credit monitoring, financial applications, and even other applications/accounts that may be attacked) for fraudulent activity. Plaintiffs, in great distress, are attempting to change their passwords and associated accounts which may be connected to various pieces of stolen PII. Plaintiffs have been monitoring their credit activity, living in constant fear and apprehension of further attacks.

Overpayment for the Products

51. Plaintiffs and the Class would not have purchased the products that led to their account creation if they knew that doing so would result in their PII being compromised and exfiltrated. Thus, they significantly overpaid based on what the products were represented to be compared to what they actually received.

Threat of Identity Theft

52. As a direct and proximate result of Defendant's breach of confidence, and failure to protect the PII, Plaintiffs and the Class have also been injured by facing ongoing, imminent,

impending threats of identity theft crimes, fraud, scams, and other misuse of this PII, resulting in ongoing monetary loss and economic harm, loss of value of privacy and confidentiality of the stolen PII, illegal sales of the compromised PII on the black market, mitigation expenses and time spent on credit monitoring, identity theft insurance, credit freezes/unfreezes, expenses and time spent in initiating fraud alerts, contacting third parties; decreased credit scores, lost work time, and other injuries. Defendant, through its misconduct, has enabled numerous bad actors to sell and profit off of PII that belongs to Plaintiffs.

53. But for Defendant's unlawful conduct, scammers would not have access to Plaintiffs' and the Class members' contact information. Defendant's unlawful conduct has directly and proximately resulted in widespread digital attacks against Plaintiffs and the Class.

Out of Pocket Costs

54. Plaintiffs are now forced to research and subsequently acquire credit monitoring and reasonable identity theft defensive services and maintain these services to avoid further impact. Plaintiffs anticipate spending out of pocket expenses to pay for these services.

55. Defendant also used Plaintiffs' PII for profit, and continued to use Plaintiffs' PII to target Plaintiffs, and share their information with various third parties for Defendant's own benefit.

Summary of Actual Economic and Noneconomic Damages

56. In sum, Plaintiffs and similarly situated consumers were injured as follows:

i. Theft of their PII and the resulting loss of privacy rights in that information;

ii. Improper disclosure of their PII;

iii. Loss of value of their PII;

iv. The amount of ongoing reasonable identity defense and credit monitoring services made necessary as mitigation measures;

v. Defendant's retention of profits attributable to Plaintiffs' and other customers' PII that Defendant failed to adequately protect;

vi. Economic and non-economic impacts that flow from imminent, and ongoing threat of fraud and identity theft to which Plaintiffs are now exposed to;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

vii. Ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of this data breach;

viii. Overpayments of Defendant's products and/or services which Plaintiffs purchased;

ix. Emotional distress, and fear associated with the imminent threat of harm from the continued phishing scams and attacks as a result of this data breach.

V. CLASS ALLEGATIONS

57. Plaintiffs bring this action on their own behalf and on behalf of all other persons similarly situated. The Class which Plaintiffs seek to represent comprises:

> "All persons who purchased or used Samsung products and services in the United States and whose PII was accessed, compromised, or stolen in the data breach announced by Samsung on September 2, 2022."

Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

58. The California Subclass which Plaintiffs seek to represent comprises:

> "All persons who purchased or used Samsung products and services in the California and whose PII was accessed, compromised, or stolen in the data breach announced by Samsung on September 2, 2022" (the "California Subclass").

Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

59. The Michigan Subclass which Plaintiffs seek to represent comprises:

> "All persons who purchased or used Samsung products and services in Michigan and whose PII was accessed, compromised, or stolen in the data breach announced by Samsung on September 2, 2022" (the "Michigan Subclass").

Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a class certification hearing, and orders of this Court.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

60. The Class is comprised of millions of consumers throughout the United States and the states of California and Michigan. The Class is so numerous that joinder of all members is impracticable and the disposition of their claims in a class action will benefit the parties and the Court.

61. There is a well-defined community of interest in the questions of law and fact involved affecting the parties to be represented in that the Class was exposed to the same common and uniform false and misleading advertising and omissions. The questions of law and fact common to the Class predominate over questions which may affect individual Class members. Common questions of law and fact include, but are not limited to, the following:

a. Whether Defendant's conduct is an unlawful business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

b. Whether Defendant's conduct is an unfair business act or practice within the meaning of Business and Professions Code section 17200, *et seq*.;

c. Whether Defendant's advertising as to their security practices is untrue or misleading within the meaning of Business and Professions Code section 17500, *et seq*.;

d. Whether Defendant's conduct is in violation of California Civil Code Sections 1709, 1710;

e. Whether Defendant's actions violate Michigan Comp. Laws Ann. Sections 445.72 and 225.903, *et seq*;

f. Whether Defendant's failure to implement effective security measures to protect Plaintiffs' and the Class' PII negligent;

g. Whether Defendant breached express and implied warranties of security to the Class;

h. Whether Defendant represented to Plaintiffs and the Class that they would protect Plaintiffs' and the Class members' PII;

i. Whether Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

j. Whether Defendant breached a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

k. Whether Class members' PII was accessed, compromised, or stolen in the breach;

l. Whether Defendant's conduct caused or resulted in damages to Plaintiffs and the Class;

m. Whether Defendant failed to notify the public of the breach in a timely and adequate manner;

n. Whether Defendant knew or should have known that its systems were vulnerable to a data breach;

o. Whether Defendant adequately addressed the vulnerabilities that allowed for the data breach; and

p. Whether, as a result of Defendant's conduct, Plaintiffs and the Class are entitled to damages and relief.

62. Plaintiffs' claims are typical of the claims of the proposed Class, as Plaintiffs and the members of the Class were harmed by Defendant's uniform unlawful conduct.

63. Plaintiffs will fairly and adequately represent and protect the interests of the proposed Class. Plaintiffs have retained competent and experienced counsel in class action and other complex litigation.

64. Plaintiffs and the Class have suffered injury in fact as a result of Defendant's false, deceptive, and misleading representations.

65. Plaintiffs would not have created a Samsung account but for the reasonable belief that Defendant would safeguard their data and PII.

66. The Class is identifiable and readily ascertainable. Notice can be provided to such purchasers using techniques and a form of notice similar to those customarily used in class actions, and by internet publication, radio, newspapers, and magazines.

67. A class action is superior to other available methods for fair and efficient adjudication of this controversy. The expense and burden of individual litigation would make it impracticable or impossible for proposed members of the Class to prosecute their claims individually.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

68. The litigation and resolution of the Class's claims are manageable. Individual litigation of the legal and factual issues raised by Defendant's conduct would increase delay and expense to all parties and the court system. The class action device presents far fewer management difficulties and provides the benefits of a single, uniform adjudication, economies of scale, and comprehensive supervision by a single court.

69. Defendant has acted on grounds generally applicable to the entire Class, thereby making final injunctive relief and/or corresponding declaratory relief appropriate with respect to the Class as a whole. The prosecution of separate actions by individual Class members would create the risk of inconsistent or varying adjudications with respect to individual member of the Class that would establish incompatible standards of conduct for Defendant.

70. Absent a class action, Defendant will likely retain the benefits of its wrongdoing. Because of the small size of the individual Class members' claims, few, if any, Class members could afford to seek legal redress for the wrongs complained of herein. Absent a representative action, the Class members will continue to suffer losses and Defendant (and similarly situated companies) will be allowed to continue these violations of law and to retain the proceeds of its ill-gotten gains.

COUNT ONE

VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW

BUSINESS & PROFESSIONS CODE SECTION 17200, *et seq.*

(ON BEHALF OF THE CALIFORNIA SUBCLASS AND NATIONWIDE CLASS)

71. Plaintiffs, individually and on behalf of the Class, herein repeat, reallege and fully incorporate all allegations in all preceding paragraphs.

72. For all Class members outside of the California and Michigan Subclasses, these claims are brought under the relevant consumer protection statute for the state in which they reside. For each state, the relevant statutes are as follows: Alabama—Deceptive Trade Practices Act (Ala. Code § 8-19-1, *et seq.*); Alaska—Unfair Trade Practices and Consumer Protection Act (Alaska Stat. § 45.50.471, *et seq.*); Arizona—Consumer Fraud Act (Ariz. Rev. Stat. Ann. § 44-1521, *et seq.*); Arkansas—Deceptive Trade Practices Act (Ark. Code Ann. § 4-88-101, *et seq.*); Colorado—Consumer Protection Act (Colo. Rev. Stat. § 6-1-101, *et seq.*); Connecticut—Connecticut Unfair

Trade Practices Act (Conn. Gen. Stat. § 42-110a, *et seq.*); Delaware—Consumer Fraud Act (Del. Code Ann. tit. 6, § 2511, *et seq.*); District of Columbia—D.C. Code § 28-3901, *et seq.*; Florida—Deceptive and Unfair Trade Practices Act (Fla. Stat. § 501.20, *et seq.*); Georgia—Fair Business Practices Act (Ga. Code Ann. § 10-1-390, *et seq.*); Hawaii—Haw. Rev. Stat. § 480-1, *et seq.*); Idaho—Consumer Protection Act (Idaho Code Ann. § 48-601, *et seq.*); Illinois—Consumer Fraud and Deceptive Business Practices Act (815 Ill. Comp. Stat. 505/1, *et seq.*); Indiana—Deceptive Consumer Sales Act (Ind. Code § 24-5-0.5-1, *et seq.*); Iowa—Iowa Code § 7.14.16, *et seq.*); Kansas—Consumer Protection Act (Kan. Stat. Ann. § 50-623, *et seq.*); Kentucky—Consumer Protection Act (Ky. Rev. Stat. Ann. § 367.110, *et seq.*); Louisiana—Unfair Trade Practices and Consumer Protection Law (La. Rev. Stat. Ann. § 51:1401, *et seq.*); Maine—Unfair Trade Practices Act (Me. Rev. Stat. Ann. tit. 5, § 205A, *et seq.*); Maryland—Maryland Consumer Protection Act (Md. Code Ann., Com. Law § 13-101, *et seq.*); Massachusetts—Regulation of Business Practice and Consumer Protection Act (Mass. Gen. Laws Ann. ch. 93A, §§ 1-11); Minnesota—False Statement in Advertising Act (Minn. Stat. § 8.31, Minn. Stat. § 325F.67), Prevention of Consumer Fraud Act (Minn. Stat. § 325F.68, *et seq.*); Mississippi—Consumer Protection Act (Miss. Code Ann. § 75-24, *et seq.*); Missouri—Merchandising Practices Act (Mo. Rev. Stat. § 407.010, *et seq.*); Montana—Unfair Trade Practices and Consumer Protection Act (Mont. Code. Ann. § 30-14-101, *et seq.*); Nebraska—Consumer Protection Act (Neb. Rev. Stat. § 59-1601); Nevada—Trade Regulation and Practices Act (Nev. Rev. Stat. § 598.0903, *et seq.*, Nev Rev. Stat. § 41.600); New Hampshire—Consumer Protection Act (N.H. Rev. Stat. Ann. § 358-A:1, *et seq.*); New Jersey—N.J. Stat. Ann. § 56:8-1, *et seq.*); New Mexico—Unfair Practices Act (N.M. Stat. § 57-12-1, *et seq.*); New York—N.Y. Gen. Bus. Law §§ 349, 350, N.Y. Exec. Law § 63(12); North Carolina—N.C. Gen. Stat. § 75-1.1, *et seq.*); North Dakota—N.D. Cent. Code § 51-15-01, *et seq.*); Ohio—Consumer Sales Practices Act (Ohio Rev. Code Ann. § 1345.01, *et seq.*); Oklahoma—Consumer Protection Act (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon—Unlawful Trade Practices Law (Or. Rev. Stat. § 646.605, *et seq.*); Pennsylvania—Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat. Ann. § 201-1, *et seq.*); Rhode Island—Unfair Trade Practice and Consumer Protection Act (R.I. Gen. Laws § 6-13.1-1, *et seq.*); South Carolina—Unfair Trade Practices Act (S.C. Code Ann. § 39-

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

5-10, *et seq.*); South Dakota—Deceptive Trade Practices and Consumer Protection Law (S.D. Codified Laws § 37-24-1, *et seq.*); Tennessee—Consumer Protection Act (Tenn. Code Ann. § 47-18-101, *et seq.*); Texas—Deceptive Trade Practices—Consumer Protection Act (Tex. Bus. & Com. Code Ann. § 17.41, *et seq.*); Utah—Consumer Sales Practices Act (Utah Code Ann. § 13-11-1, *et seq.*); Vermont—Consumer Fraud Act (Vt. Stat. Ann. tit. 9, § 2451, *et seq.*); Virginia—Consumer Protection Act (Va. Code Ann. § 59.1-196, *et seq.*); Washington—Consumer Protection Act (Wash. Rev. Code § 19.86.010, *et seq.*); West Virginia—W. Va. Code § 46A-6-101, *et seq.*); Wisconsin—Wis. Stat. § 100.18, 100.20; Wyoming—Consumer Protection Act (Wyo. Stat. Ann. § 40-12-101, *et seq.*).

A. "Unfair" Prong

73. Under California's Unfair Competition Law, Cal. Bus. & Prof. Code Section 17200, *et seq.*, a challenged activity is "unfair" when "any injury it causes outweighs any benefits provide to consumers and the injury is one that the consumers themselves could not reasonably avoid." *Camacho v. Auto Club of Southern California*, 142 Cal. App. 4th 1394, 1403 (2006).

74. Defendant's conduct as alleged herein does not confer any benefit to consumers. It is especially questionable why Defendant would continue to store individual's data wherein they made purchases for their devices years before the data breach. Mishandling this data and a failure to archive and purge this unnecessary data shows blatant disregard for customers' privacy and security.

75. Defendant did not need to collect the private data from its consumers to allow consumers' enhanced experiences of the products or services. It did so to track and target its customers, and monetize the use of the data to enhance its already exorbitant profits. Defendant utterly misused this data and PII.

76. Defendant's conduct as alleged herein causes injuries to consumers, who do not receive a product consistent with their reasonable expectations.

77. Defendant's conduct as alleged herein causes injuries to consumers, entrusted Defendant with their PII and whose PII was leaked as a result of Defendant's unlawful conduct.

78. Defendant's failure to implement and maintain reasonable security measures was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including the FTC Act, 15 U.S.C. §45, California's Consumer Records Act, Cal. Civ. Code §1798.81.5, and California's Consumer Privacy Act, Cal. Civ. Code § 1798.100.

79. Consumers cannot avoid any of the injuries caused by Defendant's conduct as alleged herein.

80. The injuries caused by Defendant's conduct as alleged herein outweigh any benefits.

81. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes an unfair business practice within the meaning of California Business and Professions Code Section 17200.

82. Defendant could have furthered its legitimate business interests in ways other than by unfair conduct.

83. Defendant's conduct threatens consumers by misleadingly advertising their systems as "secure" and exposing consumers' PII to hackers. Defendant's conduct also threatens other companies, large and small, who play by the rules. Defendant's conduct stifles competition and has a negative impact on the marketplace and reduces consumer choice.

84. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's wrongful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

85. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unfair business practices.

86. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs relied on and made their purchasing decision in part based on Defendant's representations regarding their security measures and trusted that Defendant would keep their PII safe and secure. Plaintiffs accordingly provided their PII to Defendant reasonably believing and expecting that their PII would be safe and secure. Plaintiffs paid an unwarranted premium for the purchased products and services . Specifically, Plaintiffs paid for products and services advertised as secure when Defendant in fact failed to institute adequate

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class would not have purchased the products and services, or would not have given Defendant their PII, had they known that their PII was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' PII. Additionally, Plaintiffs and the members of the Class seek and request an order awarding Plaintiffs and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

B. "Fraudulent" Prong

87. California Business and Professions Code Section 17200, *et seq.* considers conduct fraudulent and prohibits said conduct if it is likely to deceive members of the public. *Bank of the West v. Superior Court*, 2 Cal. 4th 1254, 1267 (1992).

88. Defendant's advertising and representations that they adequately protect consumer PII is likely to deceive members of the public into believing that Samsung can be entrusted with their PII, and that PII gathered by Samsung is not in danger of being compromised.

89. Defendant's representations about their products and services, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes fraudulent conduct.

90. Defendant knew or should have known of its fraudulent conduct.

91. As alleged in the preceding paragraphs, the material misrepresentations by Defendant detailed above constitute a fraudulent business practice in violation of California Business & Professions Code Section 17200.

92. Defendant could have implemented robust security measures to prevent the data breach but failed to do so.

93. Defendant's wrongful conduct is part of a pattern or generalized course of conduct.

94. Pursuant to Business & Professions Code Section 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its practice of false and deceptive advertising about the strength or adequacy of its security systems.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Likewise, Plaintiffs and the Class seek an order requiring Defendant to disclose such misrepresentations.

95. Plaintiffs and the Class have suffered injury in fact and have lost money as a result of Defendant's fraudulent conduct. Plaintiffs paid an unwarranted premium for the products and services. Plaintiffs would not have purchased the products, nor have used the services, if they had known that their use would put their PII at risk.

96. **Injunction**. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court compelling Defendant to implement adequate safeguards to protect consumer PII retained by Defendant. This includes, but is not limited to: improving security systems, deleting data that no longer needs to be retained by Defendant, archiving that data on secure servers, and notifying all affected consumers in a timely manner.

C. "Unlawful" Prong

97. California Business and Professions Code Section 17200, *et seq.*, identifies violations of any state or federal law as "unlawful practices that the unfair competition law makes independently actionable." *Velazquez v. GMAC Mortg. Corp.*, 605 F. Supp. 2d 1049, 1068 (C.D. Cal. 2008).

98. Defendant's unlawful conduct, as alleged in the preceding paragraphs, violates California Civil Code Section 1750, *et seq.*

99. Defendant's conduct, as alleged in the preceding paragraphs, is false, deceptive, misleading, and unreasonable and constitutes unlawful conduct.

100. Defendant has engaged in "unlawful" business practices by violating multiple laws, including California's Consumer Records Act, Cal. Civ. Code §§ 1798.81.5 (requiring reasonable data security measures) and 1798.82 (requiring timely breach notification), California's Consumers Legal Remedies Act, Cal. Civ. Code §§ 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, and California common law. Defendant failed to notify all of its affected customers regarding said breach, failed to take reasonable security measures, or comply with the FTC Act, and California common law.

101. Furthermore, Defendant failed to post the proper notice with the California Attorney General, and to date, it refuses to do so, failing to notify the affected customers, and seeking to

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

disguise the substantial and impeding threat of identity theft that it caused and continues to cause to consumers.

102. Defendant knew or should have known of its unlawful conduct.

103. As alleged in the preceding paragraphs, the misrepresentations by Defendant detailed above constitute an unlawful business practice within the meaning of California Business and Professions Code section 17200.

104. Defendant could have furthered its legitimate business interests in ways other than by its unlawful conduct.

105. All of the conduct alleged herein occurs and continues to occur in Defendant's business. Defendant's unlawful conduct is part of a pattern or generalized course of conduct repeated on approximately thousands of occasions daily.

106. Pursuant to Business and Professions Code Sections 17203, Plaintiffs and the Class seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its unlawful business practices.

107. Plaintiffs and the Class have suffered injury-in-fact and have lost money or property as a result of Defendant's unfair conduct. Plaintiffs paid an unwarranted premium for the products and services they purchased. Specifically, Plaintiffs paid for products and services advertised as secure when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiffs and the Class would not have purchased the products and services, or would not have given Defendant their PII, had they known that their PII was vulnerable to a data breach. Likewise, Plaintiffs and the members of the Class seek an order mandating that Defendant implement adequate security practices to protect consumers' PII. Additionally, Plaintiffs and the members of the Class seek and request an order awarding Plaintiff and the Class restitution of the money wrongfully acquired by Defendant by means of Defendant's unfair and unlawful practices.

//

//

//

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

COUNT TWO

VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT

CALIFORNIA CIVIL CODE SECTION 1750, *et seq.*

(ON BEHALF OF THE CALIFORNIA SUBCLASS)

108. Plaintiff Seirafi repeats and re-alleges the allegations set forth in the preceding paragraphs, and incorporates the same as if set forth herein at length.

109. The CLRA prohibits certain "unfair methods of competition and unfair or deceptive acts or practices" in connection with a sale of goods.

110. Defendant's unlawful conduct described herein was intended to increase sales to the consuming public and violated and continue to violate Section 1770(a)(5), (a)(7), and (a)(9) of the CLRA by representing that the products and services have characteristics and benefits which they do not have.

111. Defendant fraudulently deceived Plaintiff Seirafi and the California Subclass by representing that its products and services have certain characteristics, benefits, and qualities which they do not have, namely data protection and security. In doing so, Defendant intentionally misrepresented and concealed material facts from Plaintiff Seirafi and the California Subclass, specifically by advertising secure technology when Defendant in fact failed to institute adequate security measures and neglected system vulnerabilities that led to a data breach. Said misrepresentations and concealment were done with the intention of deceiving Plaintiff Seirafi and the California Subclass and depriving them of their legal rights and money.

112. Defendant's claims about the products and services led and continues to lead consumers like Plaintiff Seirafi to reasonably believe that Defendant has implemented adequate data security measures when Defendant in fact neglected system vulnerabilities that led to a data breach and enabled hackers to access consumers' PII.

113. Defendant knew or should have known that adequate security measures were not in place and that consumers' PII was vulnerable to a data breach.

114. Plaintiff Seirafi and the California Subclass have suffered injury in fact as a result of and in reliance upon Defendant's false representations.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

115. Plaintiff Seirafi and the California Subclass would not have purchased the products or used the services, or would have paid significantly less for the products and services, had they known that their PII was vulnerable to a data breach.

116. Defendant's actions as described herein were done with conscious disregard of Plaintiff's rights, and Defendant was wanton and malicious in its concealment of the same.

117. Plaintiff Seirafi and the California Subclass have suffered injury in fact and have lost money as a result of Defendant's unfair, unlawful, and fraudulent conduct. Specifically, Plaintiff Seirafi paid for products and services advertised as secure, and consequentially entrusted Defendant with his PII, when Defendant in fact failed to institute adequate security measures and neglected vulnerabilities that led to a data breach. Plaintiff Seirafi and the California Subclass would not have purchased the products and services, or would not have provided Defendant with their PII, had they known that their PII was vulnerable to a data breach.

118. Defendant should be compelled to implement adequate security practices to protect consumers' PII. Additionally, Plaintiff Seirafi and the members of the California Subclass lost money as a result of Defendant's unlawful practices.

119. At this time, Plaintiff Seirafi seeks injunctive relief under the CLRA pursuant to Cal. Civ. Code 1782(d); but he anticipates needing to amend the complaint and seek restitution.

COUNT THREE

VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

CAL. CIV. CODE SECTION 1798.150, *et seq.*

(ON BEHALF OF THE CALIFORNIA SUBCLASS)

120. Plaintiff Seirafi repeats and re-alleges the allegations set forth in the preceding paragraphs, and incorporates the same as if set forth herein at length.

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

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

//

123. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff Seirafi's and the California Subclass 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.

124. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiff Seirafi's and California Subclass Members' PII. As detailed herein, Defendant failed to do so.

125. As a direct and proximate result of Defendant's acts, Plaintiff Seirafi's and California Subclass Members' PII, including phone numbers, names, date of birth, addresses, email addresses, and precise geolocation data, was subjected to unauthorized access and exfiltration, theft, or disclosure.

126. Plaintiff Seirafi and California Subclass Members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including Plaintiff Seirafi's and California Subclass Members' PII. Plaintiff Seirafi and California Subclass Members 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.

127. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the PII under the CCPA.

128. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

129. Plaintiff Seirafi and the California Subclass seek actual pecuniary damages, including actual financial losses resulting from the unlawful data breach.

//

//

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

COUNT FOUR

DECEIT BY CONCEALMENT, CALIFORNIA CIVIL CODE SECTIONS 1709, 1710

(ON BEHALF OF THE CALIFORNIA SUBCLASS)

130. Plaintiff Seirafi herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

131. Defendant knew or should have known that its security systems were inadequate to protect the PII of its consumers. Defendant experienced another data breach just a few months prior to the breach at issue, which alerted Defendant to the inadequacy of its internal data protections. Despite this knowledge, Defendant failed to adequately bolster its security systems, and allowed the second breach to occur, this time compromising consumer PII. Further, the April 2022 data breach included full source code for authorizing and authenticating Samsung accounts, including APIs and services.[27] The leak of this source code should have put Samsung on further notice that the data of its account holders was at imminent risk.

132. Specifically, Defendant had an obligation to disclose to its consumers that its security systems were not adequate to safeguard their PII. Defendant did not do so. Rather, Defendant deceived Plaintiff Seirafi and the California Subclass by concealing the vulnerabilities in its security system.

133. Even after Defendant discovered the data breach, it concealed it, and waited nearly an entire month before announcing it to the public so they could know and take precautions against the data breach.

134. California Civil Code §1710 defines deceit as, (a) "[t]he suggestion, as a fact, of that which is not true, by one who does not believe it to be true"; (b) "[t]he assertion, as a fact, of that which is not true, by one who has no reasonable ground for believing it to be true"; (c) "[t]he suppression of a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact"; or (d) "[a] promise, made

[27] *See* Sead Fadilpasic, *Samsung Confirms Cyberattack, Says Internal Data Leaked*, TechRadar, https://www.techradar.com/news/samsung-hacked-galaxy-phones-leaked (last updated Apr. 14, 2022)

without any intention of performing it." Defendant's conduct as described herein therefore constitutes deceit of Plaintiff Seirafi and the California Subclass.

135. California Civil Code §1709 mandates that in willfully deceiving Plaintiff Seirafi and the California Subclass with intent to induce or alter their position to their injury or risk, Defendant is liable for any damage which Plaintiff Seirafi and the California Subclass thereby suffer.

136. As described above, Plaintiff Seirafi and the California Subclass have suffered significant harm as a direct and proximate result of Defendant's deceit and other unlawful conduct. Specifically, Plaintiff Seirafi and the Class have been subject to numerous attacks, including various phishing scams. Defendant is liable for these damages.

COUNT FIVE

MICHIGAN IDENTITY THEFT PROTECTION ACT,

MICH. COMP. LAWS ANN. SECTION 445.72, *et seq.*

(ON BEHALF OF THE MICHIGAN SUBCLASS)

137. Plaintiff Holtzclaw herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

138. Defendant is a business that owns or licenses computerized data that includes PII as defined by Mich. Comp. Laws Ann. §§ 445.72(1).

139. Plaintiff Holtzclaw's and Michigan Subclass members' PII fits the definition of PII outlined in Mich. Comp. Laws Ann. § 445.72(1)

140. Defendant is required to accurately and timely notify Plaintiff Holtzclaw and the Michigan Subclass members if it discovers a data breach, or receives notice of a data breach without unreasonable delay under Mich. Comp Laws Ann. § 445.72(1)

141. Because Defendant discovered a data breach in July of 2022, and was made aware that said breach included consumer PII, it had an obligation to disclose the data breach in a timely and accurate manner as mandated by Mich. Comp Laws Ann. § 445.72(4).

142. Defendant failed to disclose the data breach in a timely manner by waiting up to two months from learning about the breach, and nearly an entire month from the date it learned consumer PII was exfiltrated, and has thus violated Mich. Comp Laws Ann. § 445.72(4).

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

143. As a direct and proximate result of Defendant's violation of Mich. Comp Laws Ann. § 445.72(4), Plaintiff Holtzclaw and Michigan Subclass members suffered damages and continue to be at risk of future harm due to their exposed PII.

144. Plaintiff Holtzclaw and Michigan Subclass members seek all available relief under Mich. Comp Laws Ann. § 445.72(13), including a civil fine.

COUNT SIX

MICHIGAN CONSUMER PROTECTION ACT,

MICH. COMP LAWS ANN. SECTION 445.903, *et seq.*

(ON BEHALF OF THE MICHIGAN SUBCLASS)

145. Plaintiff Holtzclaw herein repeats, realleges, and fully incorporates all allegations in all preceding paragraphs.

146. Plaintiff Holtzclaw, Michigan Subclass members, and Defendant are "persons" as defined by Mich. Comp Laws Ann. § 445.903(d).

147. Defendant advertised, offered, or sold goods or services in Michigan and engaged in trade or commerce directly or indirectly affecting the people of Michigan, as defined by Mich. Comp Laws Ann. § 445.903(g).

148. Defendant engaged in unfair, unconscionable, and deceptive practices in the conduct of trade and commerce, in violation of Mich. Comp Laws Ann. § 445.903(1), including:

a. Representing that its goods and services have characteristics, uses, and benefits that they do not have;

b. Representing that its goods and services are of a particular standard or quality if they are of another;

c. Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer;

d. Making a representation or statement of fact material to the transaction such that a person reasonably believes the represented or suggested state of affairs to be other than it actually is;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

e. Failing to reveal facts that are material to the transaction in light of representations of fact made in a positive manner.

149. Defendant's unfair, unconscionable, and deceptive practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff Holtzclaw's and Michigan Subclass members' PII, which was a direct and proximate cause of the data breach;

b. Failing to identify and remedy foreseeable security and privacy risks and adequately improve security systems despite knowing not only the general risk of cybersecurity incidents, but also the specific vulnerability of Defendant's systems, having been breached just a few months earlier;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Holtzclaw's and Michigan Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

d. Failing to appropriately delete or erase data that was no longer required to be stored, so as not to unnecessarily risk consumer PII.

e. Misrepresenting that they would protect the privacy and confidentiality of Plaintiff Holtzclaw's and Michigan Subclass members' PII, including by implementing and maintaining reasonable security measures;

f. Misrepresenting that they would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff Holtzclaw's and Michigan Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

g. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff Holtzclaw's and Michigan Subclass members' PII; and

h. Omitting, suppressing, and concealing the material fact that they did not comply with common law and statutory duties pertaining to the security and privacy of

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Plaintiff Holtzclaw's and Michigan Subclass members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

150. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security systems and ability to protect consumers' PII.

151. Defendant intended to mislead Plaintiff Holtzclaw and Michigan Subclass members and induce them to rely on its own misrepresentations and omissions.

152. Defendant acted intentionally, knowingly, and maliciously to violate Michigan's Consumer Protection Act, and recklessly disregarded Plaintiff Holtzclaw's and Michigan Subclass members' rights. Defendant recent April 2022 data breach put it on notice that its security and privacy protections were inadequate.

153. As a direct and proximate result of Defendant's unfair, unconscionable, and deceptive practices, Plaintiff Holtzclaw and Michigan Subclass members have suffered and will continue to suffer injury, ascertainable loss of money or property, and monetary and non-monetary damages, as described herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their PII; overpayment for Defendant's products and services; loss of the value of access to their PII; and the value of identity protection services made necessary by the data breach.

154. Plaintiff Holtzclaw and the Michigan Subclass members seek all monetary and non-monetary relief allowed by law, including the greater of actual damages or $250 per Michigan Subclass member, injunctive relief, reasonable attorneys' fees, and any other relief that is just and proper.

COUNT SEVEN

NEGLIGENCE

(ON BEHALF OF THE NATIONWIDE CLASS)

155. Plaintiffs herein repeat, reallege, and fully incorporate all allegations in all preceding paragraphs.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

156. Defendant owed a duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII. This duty included but was not limited to: (a) designing, implementing, and testing security systems to ensure that consumers' PII was consistently and effectively protected; (b) implementing security systems that are compliant with state and federal mandates; (c) implementing security systems that are compliant with industry practices; and (d) promptly detecting and notifying affected parties of a data breach.

157. Defendant's duties to use reasonable care arose from several sources, including those described below. Defendant had a common law duty to prevent foreseeable harm to others, including Plaintiffs and members of the Class, who were the foreseeable and probable victims of any inadequate security practices.

158. Defendant's duties also arose under Section 5(a) of the Federal Trade Commission Act ("FTC Act") (15 USC § 45) prohibits "unfair or deceptive acts or practices in or affecting commerce." Defendant's failure to protect Plaintiffs and the Class members' PII constitutes an unfair or deceptive act or practice ("UDAP") because it (a) "causes or is likely to cause substantial injury to consumers;" (b) "cannot be reasonably avoided by consumers"; and (c) "is not outweighed by countervailing benefits to consumers or competition." As interpreted and enforced by the FTC, this includes the failure to use reasonable measures to protect consumers' PII.

159. Defendant knew or should have known that Plaintiffs and the Class members' PII is information that is frequently sought after by hackers.

160. Defendant knew or should have known that Plaintiffs and the Class members would suffer harm if their PII was leaked.

161. Defendant knew or should have known that its security systems were not adequate to protect Plaintiffs and the Class members' PII from a data breach, especially in light of the April 2022 data breach.

162. Defendant knew or should have known that adequate and prompt notice of the data breach was required such that Plaintiffs and the Class could have taken more swift and effective action to change or otherwise protect their PII. Defendant failed to provide timely notice upon discovery of the data breach. Plaintiffs and some of the Class members were informed of the data

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

breach on September 2, 2022. Defendant had learned of the data breach up to two months prior, in July 2022, and learned that consumers' PII was compromised nearly a month prior, on August 4, 2022. Defendant has yet to notify the remaining affected consumers.

163. Defendant's conduct as described above constituted an unlawful breach of its duty to exercise due care in collecting, storing, and safeguarding Plaintiffs' and the Class members' PII by failing to design, implement, and maintain adequate security measures to protect this information. Moreover, Defendant did not implement, design, or maintaining adequate measures to detect a data breach when it occurred.

164. Defendant's conduct as described above constituted an unlawful breach of its duty to provide adequate and prompt notice of the data breach.

165. Defendant and the Class entered into a special relationship when the Class members entrusted Defendant to protect their PII. Plaintiffs and the Class purchased Defendant's products and services, and in doing so provided Defendant with their PII, based upon Defendant's representations that it would implement adequate systems to secure their information. Defendant did not do so. Defendant knew or should have known that their security system was vulnerable to a data breach, especially after their system had been breached just months prior. Defendant breached their duty in this relationship to implement and maintain reasonable measures to protect the PII of the Class.

166. Plaintiffs and the Class members' PII would have remained private and secure had it not been for Defendant's wrongful and negligent breach of their duties. The leak of Plaintiffs and the Class members' PII, and all subsequent damages, was a direct and proximate result of Defendant's negligence.

167. Defendant's negligence was, at least, a substantial factor in causing the Plaintiffs' and the Class's PII to be improperly accessed, disclosed, and otherwise compromised, and in causing the Class members' other injuries because of the data breaches.

168. The damages suffered by Plaintiffs and the Class members was the direct and reasonably foreseeable result of Defendant's negligent breach of its duties to adequately design, implement, and maintain security systems to protect Plaintiffs and the Class members' PII.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Defendant knew or should have known that their security for safeguarding Plaintiffs and the Class members' PII was vulnerable to a data breach.

169. Defendant's negligence directly caused significant harm to Plaintiffs and the Class. Specifically, Plaintiffs and the Class have been subject to numerous attacks, including various phishing scams.

COUNT EIGHT

INTENTIONAL MISREPRESENTATION

(ON BEHALF OF THE NATIONWIDE CLASS)

170. Plaintiffs repeat and reallege all of the allegations contained above and incorporate the same as if set forth herein at length.

171. Defendant has represented, through online advertisements and its privacy policy, that Defendant "safeguards" all information provided by consumers, particularly "personal information."[28]

172. Defendant prominently advertises that it maintains "industry-leading security" and takes appropriate measures to protect consumers' information—specifically Defendant claims that their "holistic approach to security" ensures they "are protecting users' security and privacy at all times."[29]

173. Defendant in fact misrepresented the security of its services and products, failed to institute adequate security measures, and neglected vulnerabilities that led to a data breach of sensitive, personal information.

174. Defendant's misrepresentations regarding its security systems are material to a reasonable consumer, as they relate to the privacy of consumers' PII. A reasonable consumer would assign importance to such representations and would be induced to act thereon in making his or her purchase decision.

175. At all relevant times when such misrepresentations were made, Defendant knew or should have known that the representations were misleading.

[28] *See Samsung Privacy Policy for the U.S.*, SAMSUNG, https://www.samsung.com/us/account/privacy-policy/ (last updated Oct. 1, 2021).

[29] *See Samsung Mobile Security*, SAMSUNG, https://security.samsungmobile.com/main.smsb

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

176. Defendant intended for Plaintiffs and the Class to rely on the representations of its security systems, as evidenced by Defendant's intentional marketing of safe and secure services and products.

177. Plaintiffs and members of the Class reasonably and justifiably relied on Defendant's intentional misrepresentations when purchasing the products and services, and had they known the truth, they would not have purchased the products and services or would not have given Defendant their PII.

178. Defendant was negligent in its representations that it would provide the highest level of security for consumers.

179. As a direct and proximate result of Defendant's intentional misrepresentations, Plaintiffs and members of the Class have suffered injury in fact.

COUNT NINE

BREACH OF EXPRESS WARRANTY

(ON BEHALF OF THE NATIONWIDE CLASS)

180. Plaintiffs repeat and reallege the allegations set forth above and incorporate the same as if set forth herein at length.

181. Defendant made an express warranty to Plaintiffs and members of the Class that it has "industry-leading security," that "security and privacy are at the core of what [they] do and what [they] think about every day," that they maintain "safeguards designed to protect personal information, " and that its "holistic approach to security" ensures that they "are protecting users' security and privacy at all times." In order to purchase the products and services, Plaintiffs and the Class were required to provide their personal information which they reasonably believed, based on Defendant's expressed advertising claims, that it would be kept private and secure.

182. Defendant's express warranty regarding its security standards it made to Plaintiffs and the Class appears throughout its website.[30] The promises of security associated with the products and services describes the products and services, specifically relates to the products/services being purchased, and therefore becomes the basis of the bargain.

[30] *See supra* notes 4-5.

183. Plaintiffs and the Class purchased the products and services with the expectation that the information they provided would be kept safe, secure, and private in accordance with the express warranties made by Defendant on its website.

184. Defendant breached the express warranty made to Plaintiffs and Class members by failing to provide adequate security to safeguard Plaintiffs' and the Class's PII. As a result, Plaintiffs and members of the Class suffered injury and deserve to be compensated for the damages they suffered.

185. Plaintiffs and the members of the Class paid money for the products and services. However, Plaintiffs and Class members did not obtain the full value of the advertised products and services. If Plaintiffs and other Class members had known that their PII would be exposed, then they would not have purchased the products and services.

186. Plaintiffs and the Class are therefore entitled to recover all available remedies for said breach.

COUNT TEN

BREACH OF IMPLIED WARRANTY

(ON BEHALF OF THE NATIONWIDE CLASS)

187. Plaintiffs repeat and reallege the allegations set forth above and incorporate the same as if set forth herein at length.

188. Unless excluded or modified, a warranty that a good shall be merchantable is implied in a contract for their sale, if the seller is a merchant with respect to goods of that kind.

189. Defendant is a merchant with respect to the product and services, as it provides electronic products and services, including but not limited to, mobile phones, smartphones, televisions, printers, and semiconductor chips. In exchange, Defendant receives benefits in the form of monetary payments and/or other valuable consideration, *e.g.*, access to consumers' private and personal data.

190. In using Defendant's products and services, Plaintiffs and the Class continually provide Defendant with their valuable private and personal information.

191. Defendant acknowledged these benefits and accepted or retained them.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

192. Defendant was obligated to take reasonable steps to secure and safeguard Plaintiffs' and the Class Members' sensitive information.

193. All parties understood that such security was an integral and essential Defendant's products and services.

194. Defendant breached the implied warranty of merchantability to Plaintiffs and the Class in its representations that the purchased product and services would maintain the security of their PII. Contrary to the promise and affirmation of fact, Defendant failed to provide such security.

195. As a result of Defendant's conduct, Plaintiffs and the Class did not receive merchantable goods and services as impliedly warranted by Defendant.

196. Defendant did not exclude or modify the products and services implied warranty of merchantability.

197. As a proximate result of Defendant's breach of its implied warranty, Plaintiffs and members of the Class incurred damages. Plaintiffs and members of the Class were damaged as a result of Defendant's failure to comply with its obligations under the implied warranty, since Plaintiffs and members of the Class paid for a product that did not have the promised quality and nature, did not receive the services that they bargained for, paid a premium for the product/service when they could have instead purchased other less expensive alternative products/services, and lost the opportunity to purchase other similar products/services.

198. Plaintiffs and the Class are therefore entitled to recover all available remedies for said breach.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for judgment and relief on all cause of action as follows:

A. That the Court determines that this Action may be maintained as a Class Action, that Plaintiffs be named as Class Representatives of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

B. That the Court enter an order declaring that Defendant's actions, as set forth in this Complaint, violate the laws set forth above;

C. An order:

a. Prohibiting Defendant from engaging in the wrongful acts stated herein (including Defendant's utter failure to provide notice to all affected consumers);

b. Requiring to implement adequate security protocols and practices to protect consumers' PII consistent with the industry standards, applicable regulations, and federal, state, and/or local laws;

c. Mandating the proper notice be sent to all affected consumers, and posted publicly;

d. Requiring Defendant to protect all data collected through its account creation requirements;

e. Requiring Defendant to delete, destroy, and purge the PII of Plaintiffs and Class Members unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

f. Requiring Defendant to implement and maintain a comprehensive security program designed to protect the confidentiality and integrity of Plaintiffs' and Class Members' PII;

g. Requiring Defendant to engage independent third-party security auditors and conduct internal security audit and testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis;

h. Requiring Defendant to engage independent third-party security auditors and/or internal personnel to run automated security monitoring;

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

i. Requiring Defendant to create the appropriate firewalls, and implement the necessary measures to prevent further disclosure and leak of any additional information;

j. Requiring Defendant to conduct systematic scanning for data breach related issues;

k. Requiring Defendant to train and test its employees regarding data breach protocols, archiving protocols, and conduct any necessary employee background checks to ensure that only individuals with the appropriate training and access may be allowed to access the PII data; and

l. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

D. That the Court award Plaintiffs and the Class damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

E. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiff and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

F. That the Court award Plaintiffs and the Class pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

G. That the Court award Plaintiffs and the Class their reasonable attorneys' fees and costs of suit;

H. That the Court award treble and/or punitive damages insofar as they are allowed by applicable laws; and

I. That the Court award any and all other such relief as the Court may deem just and proper under the circumstances.

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs respectfully demand a trial by jury for all claims.

DATED: September 9, 2022

CLARKSON LAW FIRM, P.C.

/s/ Yana Hart
Ryan J. Clarkson, Esq.
Katherine A. Bruce, Esq.
Bahar Sodaify, Esq.
Yana Hart, Esq.

TYCKO & ZAVAREEI LLP
Sabita J. Soneji, Esq.
Hassan A. Zavareei, Esq.

Attorneys for Plaintiffs

Clarkson Law Firm, P.C. | 22525 Pacific Coast Highway | Malibu, CA 90265