

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

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

8 I. INTRODUCTION

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

21
 22
 23 ¹ See Kim Eun-jin, *Samsung Electronics Ranked 4th in Forbes’ List of World’s Largest Tech*
 24 *Companies*, BUSINESS KOREA (May 16, 2022, 4:48 PM),
<http://www.businesskorea.co.kr/news/articleView.html?idxno=92787>.

25 ² See *Samsung Privacy Policy for the U.S.*, SAMSUNG,
<https://www.samsung.com/us/account/privacy-policy/> (last updated Oct. 1, 2021).

26 ³ *Id.*

27 ⁴ See *Welcome to Samsung Mobile Security*, SAMSUNG MOBILE SECURITY,
<https://security.samsungmobile.com/main.smsb> (last visited September 8, 2022).

28 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).

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

3 “[W]e recognize the importance of protecting our users’ security and privacy.”⁷

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

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

10 **II. PARTIES**

11 3. Plaintiff Seirafi is an individual residing in California, who had his personal
12 identifiable information (“PII”) exfiltrated and compromised in the data breach *announced* by
13 Defendant on September 2, 2022. Seirafi purchased two Samsung printers, one online in September
14 of 2015, and one at a BestBuy store in California in 2018. To gain access to certain features such as
15 software drivers and the printer application for MacOS, Seirafi was required to create a Samsung
16 account and register the devices. Seirafi created an account and registered both devices on October
17 2, 2018. In doing so, Seirafi was required to provide Defendant with his name, postal address, email
18 address, date of birth, and phone number, among other information. In making his decision to create
19 a Samsung account to gain full access to the products’ features, Seirafi reasonably expected that
20 Defendant would safeguard his PII. Seirafi would not have purchased the products, nor would he
21 have created a Samsung account, if he knew that the sensitive information collected by Defendant
22 would be at risk. Seirafi has suffered damages and remains at a significant risk now that his PII has
23 been leaked online.

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

26
27 ⁶ *Welcome to Samsung Mobile Security*, SAMSUNG MOBILE SECURITY,
<https://security.samsungmobile.com/main.smsb> (last visited September 8, 2022).

28 ⁷ *Id.*

⁸ *Id.*

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

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

19 **III. JURISDICTION AND VENUE**

20 6. This Court has subject matter jurisdiction of this action pursuant to 28 U.S.C. Section
21 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more class members,
22 (ii) there is an aggregate amount in controversy exceeding \$5,000,000, exclusive of interest and
23 costs, and (iii) there is minimal diversity because at least one Plaintiff (CA) and Defendant (NY,
24 NJ) are citizens of different states. This Court has supplemental jurisdiction over any state law
25 claims pursuant to 28 U.S.C. Section 1367.

26
27 _____
28 ⁹ Saurabh Sharma, LINKEDIN, (accessed on September 9, 2022),
<https://www.linkedin.com/in/saurabh-sharma-9b0aa38/>

¹⁰ *Id.*

1 7. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action
2 because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred
3 in this District: Defendant's decision making processes affecting data and privacy stem from its San
4 Francisco offices, Defendant markets and sells products and services in this District, Defendant
5 gains revenue and profits from doing business in this District, consumers sign up for Samsung
6 accounts and provide Samsung with their PII in this District, Class members affected by the breach
7 reside in this District, Defendant has a corporate office in this District, and Defendant employs
8 numerous people in this District, a number of whom work specifically on making decisions
9 regarding the data privacies and handling of consumers' data.

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

17 **IV. FACTUAL ALLEGATIONS**

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

23 10. Defendant collects and processes the personal data of millions of consumers,
24 including personal information obtained across all of Samsung's Internet-connected Samsung
25 devices and services (from mobile phones and tablets to TVs, home appliances, online services, and
26

27 ¹¹ *Samsung Revenue: Sales, Manufacturing, Employees / 2012-2022*, MIRROR MEISTER (Jan. 1,
28 2021), <https://www.mirrormeister.com/samsung-revenue-productions-stats/>.

¹² *Id.*

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

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

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

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

23 14. The information collected and stored by Defendant includes, but is not limited to,
24 ***names, dates of birth, addresses, precise geolocation data, email addresses, phone numbers, and***
25 ***information about the products each consumer owns***. Defendant collected this PII by requiring
26

27 _____
¹³ See *supra* note 2.

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

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

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

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

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

14 **Our approach to privacy**

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

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

21 When you use Samsung products or services, you may provide information about who you are, who you call or
22 text, what shows you watch, or what you view online. **We recognize the importance of protecting your
23 information. Our products and services are designed with privacy and security at top of mind.** Let us tell
24 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
25 used without permission, lost or stolen. Features such as fingerprint, facial and iris authentication to help ensure
26 that you, and only you, can access and use your phone.

Knox & Privacy: **the protection of your personal data is underwritten by industry leading
27 security. Samsung has developed a defense-grade security solution called Knox that is built into the
28 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)

1 currently available. This technology is not just for mobile devices. It can be the key to securing information
2 traveling through connected devices in the world of the Internet of Things (IoT).

3 Payments & Privacy: our digital wallet, Samsung Pay, incorporates a technology called tokenization that means
4 you don't use your actual credit card number for payment transactions, and enables you to use your phone with
5 little worry that your account numbers will be exposed.

6 SmartTVs & Privacy: **we've embedded encryption on our TVs for the storage and transmission of your
7 information whenever you use apps or surf the internet.**

8 Appliances: Connected appliances such as our Family Hub refrigerators use information you provide to enable
9 features such as calendar sharing and shopping list. These devices also feature services that allow you to order
10 products through third parties. the data is protected with industry standard encryption to help protect your
11 information.

12 These are some of the ways that **we have sought to empower you, our customer, to protect yourself and your
13 information.** We would be remiss if we didn't also talk to you about how we use information that you choose to
14 give to us when you enjoy our products and services.

15 Our priority as a company is to utilize information to enhance your customer experience with our products and
16 services. We challenge ourselves to think of you first and our innovation is driven by how people use our
17 products. We use data to inform ourselves about what you use and like, and what you are not so crazy
18 about. Delivering to you, our customer, a personalized, seamless experience that you find valuable can only be
19 crafted if we know what works for you. So we provide notices to you about the types of information that are used
20 in order to deliver that seamless experience.

21 Innovation is continually changing and so do privacy implications that accompany it. As such, we are constantly
22 looking for ways to improve our interaction with you by seeking to strike the right balance between protecting
23 your privacy while providing the best possible experience. That is our enduring commitment.¹⁷

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

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

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

23 ¹⁸ *Important Notice Regarding Customer Information*, SAMSUNG (Sept. 2, 2022),
24 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.

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

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

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

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

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

22 **FIRST DATA BREACH**

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

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

27 _____
28 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>.

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

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

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

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

SECOND DATA BREACH

24 30. Defendant once again failed to implement any effective security measures to prevent
25 a data breach, leading to its second, and most current, data breach. Indeed, despite Defendant’s full
26

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

28 ²¹ *Id.*

²² *Id.*

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

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

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

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

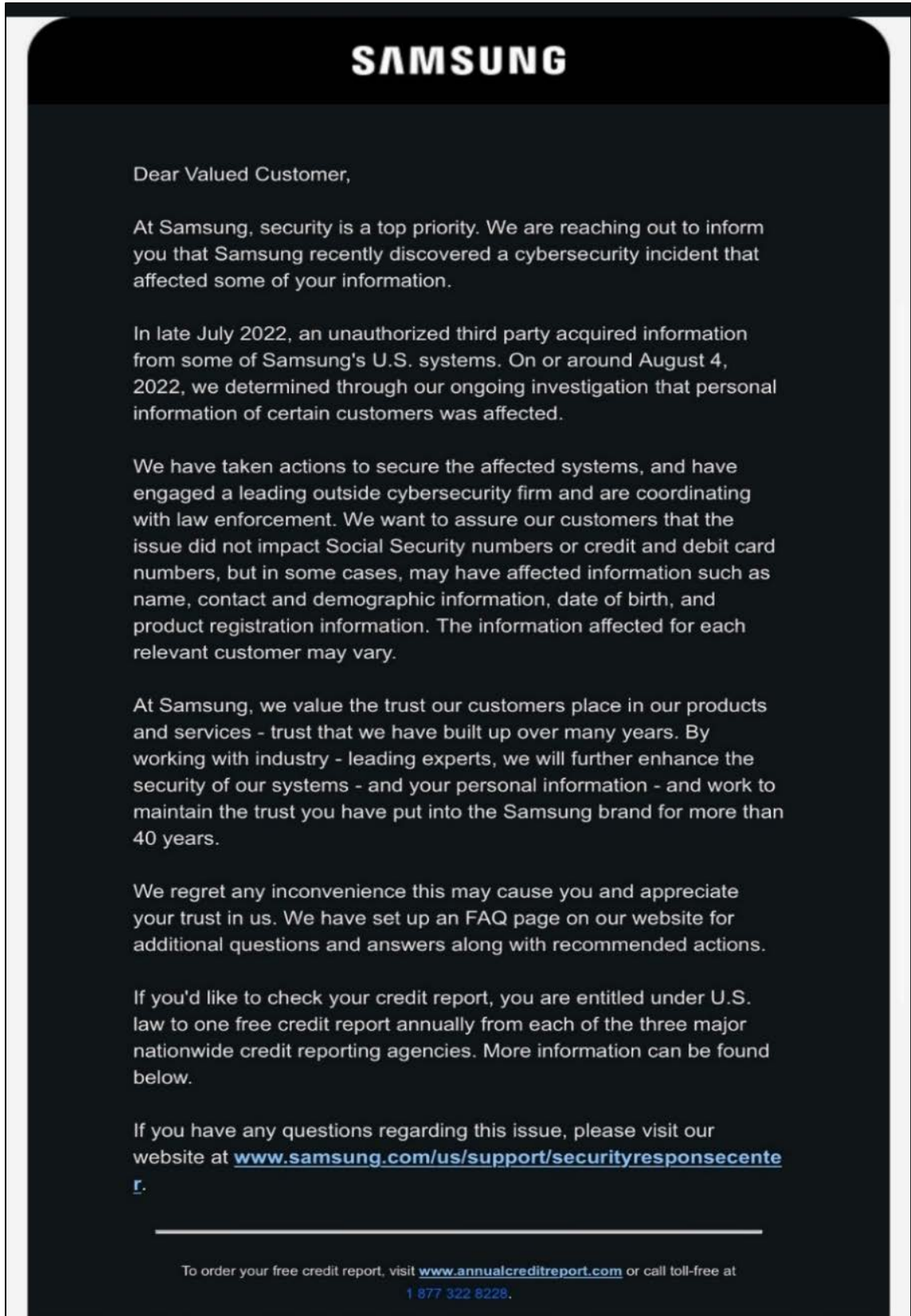
15 34. To date, Defendant fails to explain the scope of this breach, or notify all affected
 16 customers.

17 35. Defendant confirmed that this PII included “information such as name, contact and
 18 demographic information, date of birth, and product registration information.”²³

19 36. Nevertheless, despite **knowing** about this attack as of August 4, 2022, Defendant did
 20 not release a statement to affected consumers until September 2, 2022, *up to two months after* the
 21 breach happened, and *nearly an entire month* after they became aware that consumers’ data had
 22
 23
 24
 25

26 ²³ *Important Notice Regarding Customer Information*, SAMSUNG (Sept. 2, 2022),
 27 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.
 28

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



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

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

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

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

11 **IMPACT OF DATA BREACH ON CONSUMERS**

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

21 **Digital Phishing Scams**

22 41. Phishing scammers use emails and text messages to trick people into giving them their
23 personal information, including but not limited to passwords, account numbers, and social security
24

25
26
27 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/>.

28 ²⁵ See U.S. GOV'T ACCOUNTABILITY OFF. REPORT TO CONGRESSIONAL REQUESTERS 29 2007.
<https://www.gao.gov/new.items/d07737.pdf>.

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

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

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

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

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

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

27 _____
28 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).

1 **SIM-Swap**

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

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

10 **Loss of Time**

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

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

21 **Overpayment for the Products**

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

26 **Threat of Identity Theft**

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

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

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

11 **Out of Pocket Costs**

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

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

17 **Summary of Actual Economic and Noneconomic Damages**

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

- 19 i. Theft of their PII and the resulting loss of privacy rights in that information;
- 20 ii. Improper disclosure of their PII;
- 21 iii. Loss of value of their PII;
- 22 iv. The amount of ongoing reasonable identity defense and credit monitoring services
23 made necessary as mitigation measures;
- 24 v. Defendant's retention of profits attributable to Plaintiffs' and other customers' PII
25 that Defendant failed to adequately protect;
- 26 vi. Economic and non-economic impacts that flow from imminent, and ongoing
27 threat of fraud and identity theft to which Plaintiffs are now exposed to;
- 28

- 1 vii. Ascertainable out-of-pocket expenses and the value of their time allocated to
- 2 fixing or mitigating the effects of this data breach;
- 3 viii. Overpayments of Defendant’s products and/or services which Plaintiffs
- 4 purchased;
- 5 ix. Emotional distress, and fear associated with the imminent threat of harm from the
- 6 continued phishing scams and attacks as a result of this data breach.

7 **V. CLASS ALLEGATIONS**

8 57. Plaintiffs bring this action on their own behalf and on behalf of all other persons

9 similarly situated. The Class which Plaintiffs seek to represent comprises:

10 “All persons who purchased or used Samsung products and

11 services in the United States and whose PII was accessed,

12 compromised, or stolen in the data breach announced by

13 Samsung on September 2, 2022.”

14 Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a

15 class certification hearing, and orders of this Court.

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

17 “All persons who purchased or used Samsung products and

18 services in the California and whose PII was accessed,

19 compromised, or stolen in the data breach announced by

20 Samsung on September 2, 2022” (the “California Subclass”).

21 Said definition may be further defined or amended by additional pleadings, evidentiary hearings, a

22 class certification hearing, and orders of this Court.

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

24 “All persons who purchased or used Samsung products and services in Michigan and

25 whose PII was accessed, compromised, or stolen in the data breach announced by

26 Samsung on September 2, 2022” (the “Michigan Subclass”).

27 Said definition may be further defined or amended by additional pleadings, evidentiary

28 hearings, a class certification hearing, and orders of this Court.

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

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

- 10 a. Whether Defendant's conduct is an unlawful business act or practice within the
11 meaning of Business and Professions Code section 17200, *et seq.*;
- 12 b. Whether Defendant's conduct is an unfair business act or practice within the
13 meaning of Business and Professions Code section 17200, *et seq.*;
- 14 c. Whether Defendant's advertising as to their security practices is untrue or
15 misleading within the meaning of Business and Professions Code section 17500,
16 *et seq.*;
- 17 d. Whether Defendant's conduct is in violation of California Civil Code Sections
18 1709, 1710;
- 19 e. Whether Defendant's actions violate Michigan Comp. Laws Ann. Sections 445.72
20 and 225.903, *et seq.*;
- 21 f. Whether Defendant's failure to implement effective security measures to protect
22 Plaintiffs' and the Class' PII negligent;
- 23 g. Whether Defendant breached express and implied warranties of security to the
24 Class;
- 25 h. Whether Defendant represented to Plaintiffs and the Class that they would protect
26 Plaintiffs' and the Class members' PII;
- 27 i. Whether Defendant owed a duty to Plaintiffs and the Class to exercise due care in
28 collecting, storing, and safeguarding their PII;

- 1 j. Whether Defendant breached a duty to Plaintiffs and the Class to exercise due care
- 2 in collecting, storing, and safeguarding their PII;
- 3 k. Whether Class members' PII was accessed, compromised, or stolen in the breach;
- 4 l. Whether Defendant's conduct caused or resulted in damages to Plaintiffs and the
- 5 Class;
- 6 m. Whether Defendant failed to notify the public of the breach in a timely and
- 7 adequate manner;
- 8 n. Whether Defendant knew or should have known that its systems were vulnerable
- 9 to a data breach;
- 10 o. Whether Defendant adequately addressed the vulnerabilities that allowed for the
- 11 data breach; and
- 12 p. Whether, as a result of Defendant's conduct, Plaintiffs and the Class are entitled
- 13 to damages and relief.

14 62. Plaintiffs' claims are typical of the claims of the proposed Class, as Plaintiffs and the

15 members of the Class were harmed by Defendant's uniform unlawful conduct.

16 63. Plaintiffs will fairly and adequately represent and protect the interests of the proposed

17 Class. Plaintiffs have retained competent and experienced counsel in class action and other complex

18 litigation.

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

20 deceptive, and misleading representations.

21 65. Plaintiffs would not have created a Samsung account but for the reasonable belief that

22 Defendant would safeguard their data and PII.

23 66. The Class is identifiable and readily ascertainable. Notice can be provided to such

24 purchasers using techniques and a form of notice similar to those customarily used in class actions,

25 and by internet publication, radio, newspapers, and magazines.

26 67. A class action is superior to other available methods for fair and efficient adjudication

27 of this controversy. The expense and burden of individual litigation would make it impracticable or

28 impossible for proposed members of the Class to prosecute their claims individually.

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

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

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

16 **COUNT ONE**

17 **VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW**

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

19 **(ON BEHALF OF THE CALIFORNIA SUBCLASS AND NATIONWIDE CLASS)**

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

22 72. For all Class members outside of the California and Michigan Subclasses, these claims
23 are brought under the relevant consumer protection statute for the state in which they reside. For
24 each state, the relevant statutes are as follows: Alabama—Deceptive Trade Practices Act (Ala. Code
25 § 8-19-1, et seq.); Alaska—Unfair Trade Practices and Consumer Protection Act (Alaska Stat. §
26 45.50.471, et seq.); Arizona—Consumer Fraud Act (Ariz. Rev. Stat. Ann. § 44-1521, et seq.);
27 Arkansas—Deceptive Trade Practices Act (Ark. Code Ann. § 4-88-101, et seq.); Colorado—
28 Consumer Protection Act (Colo. Rev. Stat. § 6-1-101, et seq.); Connecticut—Connecticut Unfair

1 Trade Practices Act (Conn. Gen. Stat. § 42-110a, *et seq.*); Delaware—Consumer Fraud Act (Del.
 2 Code Ann. tit. 6, § 2511, *et seq.*); District of Columbia—D.C. Code § 28-3901, *et seq.*; Florida—
 3 Deceptive and Unfair Trade Practices Act (Fla. Stat. § 501.20, *et seq.*); Georgia—Fair Business
 4 Practices Act (Ga. Code Ann. § 10-1-390, *et seq.*); Hawaii—Haw. Rev. Stat. § 480-1, *et seq.*);
 5 Idaho—Consumer Protection Act (Idaho Code Ann. § 48-601, *et seq.*); Illinois—Consumer Fraud
 6 and Deceptive Business Practices Act (815 Ill. Comp. Stat. 505/1, *et seq.*); Indiana—Deceptive
 7 Consumer Sales Act (Ind. Code § 24-5-0.5-1, *et seq.*); Iowa—Iowa Code § 7.14.16, *et seq.*);
 8 Kansas—Consumer Protection Act (Kan. Stat. Ann. § 50-623, *et seq.*); Kentucky—Consumer
 9 Protection Act (Ky. Rev. Stat. Ann. § 367.110, *et seq.*); Louisiana—Unfair Trade Practices and
 10 Consumer Protection Law (La. Rev. Stat. Ann. § 51:1401, *et seq.*); Maine—Unfair Trade Practices
 11 Act (Me. Rev. Stat. Ann. tit. 5, § 205A, *et seq.*); Maryland—Maryland Consumer Protection Act
 12 (Md. Code Ann., Com. Law § 13-101, *et seq.*); Massachusetts—Regulation of Business Practice
 13 and Consumer Protection Act (Mass. Gen. Laws Ann. ch. 93A, §§ 1-11); Minnesota—False
 14 Statement in Advertising Act (Minn. Stat. § 8.31, Minn. Stat. § 325F.67), Prevention of Consumer
 15 Fraud Act (Minn. Stat. § 325F.68, *et seq.*); Mississippi—Consumer Protection Act (Miss. Code
 16 Ann. § 75-24, *et seq.*); Missouri—Merchandising Practices Act (Mo. Rev. Stat. § 407.010, *et seq.*);
 17 Montana—Unfair Trade Practices and Consumer Protection Act (Mont. Code. Ann. § 30-14-101,
 18 *et seq.*); Nebraska—Consumer Protection Act (Neb. Rev. Stat. § 59-1601); Nevada—Trade
 19 Regulation and Practices Act (Nev. Rev. Stat. § 598.0903, *et seq.*, Nev. Rev. Stat. § 41.600); New
 20 Hampshire—Consumer Protection Act (N.H. Rev. Stat. Ann. § 358-A:1, *et seq.*); New Jersey—N.J.
 21 Stat. Ann. § 56:8-1, *et seq.*); New Mexico—Unfair Practices Act (N.M. Stat. § 57-12-1, *et seq.*);
 22 New York—N.Y. Gen. Bus. Law §§ 349, 350, N.Y. Exec. Law § 63(12); North Carolina—N.C.
 23 Gen. Stat. § 75-1.1, *et seq.*); North Dakota—N.D. Cent. Code § 51-15-01, *et seq.*); Ohio—Consumer
 24 Sales Practices Act (Ohio Rev. Code Ann. § 1345.01, *et seq.*); Oklahoma—Consumer Protection
 25 Act (Okla. Stat. tit. 15, § 751, *et seq.*); Oregon—Unlawful Trade Practices Law (Or. Rev. Stat. §
 26 646.605, *et seq.*); Pennsylvania—Unfair Trade Practices and Consumer Protection Law (73 Pa. Stat.
 27 Ann. § 201-1, *et seq.*); Rhode Island—Unfair Trade Practice and Consumer Protection Act (R.I.
 28 Gen. Laws § 6-13.1-1, *et seq.*); South Carolina—Unfair Trade Practices Act (S.C. Code Ann. § 39-

1 5-10, *et seq.*); South Dakota—Deceptive Trade Practices and Consumer Protection Law (S.D.
 2 Codified Laws § 37-24-1, *et seq.*); Tennessee—Consumer Protection Act (Tenn. Code Ann. § 47-
 3 18-101, *et seq.*); Texas—Deceptive Trade Practices—Consumer Protection Act (Tex. Bus. & Com.
 4 Code Ann. § 17.41, *et seq.*); Utah—Consumer Sales Practices Act (Utah Code Ann. § 13-11-1, *et*
 5 *seq.*); Vermont—Consumer Fraud Act (Vt. Stat. Ann. tit. 9, § 2451, *et seq.*); Virginia—Consumer
 6 Protection Act (Va. Code Ann. § 59.1-196, *et seq.*); Washington—Consumer Protection Act (Wash.
 7 Rev. Code § 19.86.010, *et seq.*); West Virginia—W. Va. Code § 46A-6-101, *et seq.*); Wisconsin—
 8 Wis. Stat. § 100.18, 100.20; Wyoming—Consumer Protection Act (Wyo. Stat. Ann. § 40-12-101,
 9 *et seq.*).

10 **A. “Unfair” Prong**

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

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

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

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

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

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

1 entities that are trusted with it use appropriate security measures. These policies are reflected in
2 laws, including the FTC Act, 15 U.S.C. §45, California’s Consumer Records Act, Cal. Civ. Code
3 §1798.81.5, and California’s Consumer Privacy Act, Cal. Civ. Code § 1798.100.

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

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

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

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

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

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

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

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

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

8 **B. "Fraudulent" Prong**

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

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

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

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

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

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

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

25 94. Pursuant to Business & Professions Code Section 17203, Plaintiffs and the Class
26 seek an order of this Court enjoining Defendant from continuing to engage, use, or employ its
27 practice of false and deceptive advertising about the strength or adequacy of its security systems.
28

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

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

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

12 **C. "Unlawful" Prong**

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

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

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

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

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

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

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

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

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

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

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

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

26 //

27 //

28 //

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

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

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

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

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

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

18 **COUNT THREE**

19 **VIOLATION OF CALIFORNIA CONSUMER PRIVACY ACT (“CCPA”)**

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

21 **(ON BEHALF OF THE CALIFORNIA SUBCLASS)**

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

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

26 122. Defendant collects consumers’ personal information as defined in Cal. Civ. Code §
27 1798.140.

28 //

1 123. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiff Seirafi’s
2 and the California Subclass Members’ nonencrypted PII from unauthorized access and exfiltration,
3 theft, or disclosure as a result of Defendant’s violations of its duty to implement and maintain
4 reasonable security procedures and practices appropriate to the nature of the information.

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

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

12 126. Plaintiff Seirafi and California Subclass Members seek injunctive or other equitable
13 relief to ensure Defendant hereinafter adequately safeguards customers’ PII by implementing
14 reasonable security procedures and practices. Such relief is particularly important because
15 Defendant continues to hold customers’ PII, including Plaintiff Seirafi’s and California Subclass
16 Members’ PII. Plaintiff Seirafi and California Subclass Members have an interest in ensuring that
17 their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately
18 safeguard this information, as evidenced by its multiple data breaches.

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

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

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

27 //

28 //

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)

1 without any intention of performing it.” Defendant’s conduct as described herein therefore
2 constitutes deceit of Plaintiff Seirafi and the California Subclass.

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

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

10 **COUNT FIVE**

11 **MICHIGAN IDENTITY THEFT PROTECTION ACT,**

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

13 **(ON BEHALF OF THE MICHIGAN SUBCLASS)**

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

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

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

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

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

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

1 143. As a direct and proximate result of Defendant’s violation of Mich. Comp Laws Ann.
2 § 445.72(4), Plaintiff Holtzclaw and Michigan Subclass members suffered damages and continue
3 to be at risk of future harm due to their exposed PII.

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

6 **COUNT SIX**

7 **MICHIGAN CONSUMER PROTECTION ACT,**

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

9 **(ON BEHALF OF THE MICHIGAN SUBCLASS)**

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

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

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

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

- 19 a. Representing that its goods and services have characteristics, uses, and benefits
20 that they do not have;
- 21 b. Representing that its goods and services are of a particular standard or quality if
22 they are of another;
- 23 c. Failing to reveal a material fact, the omission of which tends to mislead or
24 deceive the consumer, and which fact could not reasonably be known by the
25 consumer;
- 26 d. Making a representation or statement of fact material to the transaction such that
27 a person reasonably believes the represented or suggested state of affairs to be
28 other than it actually is;

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- 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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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.

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

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

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

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

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

22 161. Defendant knew or should have known that its security systems were not adequate to
23 protect Plaintiffs and the Class members' PII from a data breach, especially in light of the April
24 2022 data breach.

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

1 breach on September 2, 2022. Defendant had learned of the data breach up to two months prior, in
2 July 2022, and learned that consumers' PII was compromised nearly a month prior, on August 4,
3 2022. Defendant has yet to notify the remaining affected consumers.

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

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

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

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

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

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

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

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

6 **COUNT EIGHT**

7 **INTENTIONAL MISREPRESENTATION**

8 **(ON BEHALF OF THE NATIONWIDE CLASS)**

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

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

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

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

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

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

27 ²⁸ See *Samsung Privacy Policy for the U.S.*, SAMSUNG,
28 <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>

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

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

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

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

14 **COUNT TEN**

15 **BREACH OF IMPLIED WARRANTY**

16 **(ON BEHALF OF THE NATIONWIDE CLASS)**

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

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

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

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

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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;

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

- 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.

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

CIVIL COVER SHEET

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

I. (a) PLAINTIFFS

NAEEM SEIRAFI and SHELBY HOLTZCLAW

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

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

Ryan J. Clarkson, Bahar Sodaify, Yana Hart, Katherine A. Bruce
Clarkson Law Firm, P.C., 22525 Pacific Coast Highway, Malibu, CA 90265

DEFENDANTS

SAMSUNG ELECTRONICS AMERICA, INC.

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

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

Attorneys (If Known)

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

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

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

Table with columns for Plaintiff (PTF) and Defendant (DEF) citizenship and incorporation status.

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

Large table with categories: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, HABEAS CORPUS, OTHER, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES.

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

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

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
Brief description of cause:
Violations of Class Action Fairness Act ("CAFA"); consumer protection/false advertising/unfair competition state-law based claims

VII. REQUESTED IN COMPLAINT:

CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$ 5,000,001.00 CHECK YES only if demanded in complaint: JURY DEMAND: X Yes No

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

JUDGE DOCKET NUMBER

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

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

DATE 09/09/2022 SIGNATURE OF ATTORNEY OF RECORD /s/ Yana Hart

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

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

- I. a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.
 - b) **County of Residence.** For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the “defendant” is the location of the tract of land involved.)
 - c) **Attorneys.** Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section “(see attachment).”
- II. Jurisdiction.** The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an “X” in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
- (1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.
 - (2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an “X” in this box.
 - (3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
 - (4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)
- III. Residence (citizenship) of Principal Parties.** This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.
- IV. Nature of Suit.** Place an “X” in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.
- V. Origin.** Place an “X” in one of the six boxes.
- (1) Original Proceedings. Cases originating in the United States district courts.
 - (2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.
 - (3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
 - (4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
 - (5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
 - (6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.
 - (8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket. Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.
- VI. Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.
- VII. Requested in Complaint.** Class Action. Place an “X” in this box if you are filing a class action under Federal Rule of Civil Procedure 23. Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction. Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.
- VIII. Related Cases.** This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.
- IX. Divisional Assignment.** If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: “the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated.”
- Date and Attorney Signature.** Date and sign the civil cover sheet.