

1 John A. Yanchunis (Pro Hac Vice to be filed)  
 2 Ryan J. McGee (Pro Hac Vice to be filed)  
**MORGAN & MORGAN**  
**COMPLEX LITIGATION GROUP**  
 3 201 N. Franklin Street, 7th Floor  
 4 Tampa, Florida 33602  
 Telephone: (813) 223-5505  
 5 Facsimile: (813) 223-5402  
*jyanchunis@ForThePeople.com*  
 6 *rmcgee@ForThePeople.com*

7 Clayeo C. Arnold, California SBN 65070  
 8 Joshua H. Watson, California SBN 238058  
**CLAYEO C. ARNOLD, A**  
**PROFESSIONAL LAW CORPORATION**  
 9 865 Howe Avenue  
 10 Sacramento, California 95825  
 Telephone: (916) 777-7777  
 11 Facsimile: (916) 924-1829  
*carnold@justice4you.com*  
 12 *jwatson@justice4you.com*

13 *Attorneys for Plaintiffs and the Class*

14  
 15 **UNITED STATES DISTRICT COURT**  
 16 **NORTHERN DISTRICT OF CALIFORNIA**

17  
 18 MICHAEL FORD and RUDOLPH  
 19 DUBROVSZKY, individually and on behalf  
 of all others similarly situated,

20 Plaintiff,

21 v.

22 24/7, INC., a California Corporation,  
 23 BEST BUY CO., INC., a Minnesota  
 24 corporation, and DELTA AIRLINES,  
 INC., a Delaware corporation,

25 Defendants.  
 26  
 27  
 28

CASE NO.

**CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

1 Plaintiffs, Michael Ford (“Ford” or the “Best Buy Plaintiff”) and Rudolph  
2 Dubrovsky (“Dubrovsky” or the “Delta Plaintiff”), on behalf of themselves and all others  
3 similarly situated, file this Class Action Complaint against Defendants, 24/7, Inc. (“24/7”),  
4 Best Buy Co., Inc. (“Best Buy”), and Delta Airlines, Inc. (“Delta”) (collectively  
5 “Defendants”), and based upon personal knowledge with respect to themselves and on  
6 information and belief derived therefrom, among other things, investigation of counsel and  
7 review of public documents as to all other matters, allege as follows:

### 8 SUMMARY OF THE CASE

9 1. Plaintiffs bring this class action against Defendants for their failure to secure  
10 and safeguard customers’ payment card data (“PCD”) and other personally identifiable  
11 information (“PII”) that Defendants collected during customer service support contact with  
12 Best Buy and Delta , and for failing to provide timely, accurate, and adequate notice to  
13 Plaintiffs and the Class and Subclass members that their PCD and PII (hereinafter,  
14 collectively, “Customer Data”) had been compromised and stolen.

15 2. 24/7 is a customer experience software and services company headquartered  
16 in San Jose, California, with approximately 12,000 employees. 24/7 offers sales and  
17 service-oriented software, as well as voice and chat agent services, for sales and support.  
18 Best Buy and Delta have used 24/7 for such services since at least, and likely well before,  
19 September 27, 2017—the purported beginning of the data breach described herein.

20 3. Best Buy is a retail company with over 1,000 stores throughout the United  
21 States providing technology products, services, and solutions. Best Buy offers “expert  
22 service” more than 1.5 billion times every year to consumers, small business owners, and  
23 educators who visit and patronize Best Buy stores. Best Buy also provides the “Geek  
24 Squad” service to further facilitate its goal of providing technology products, services, and  
25 solutions. Best Buy markets and makes these products and services through various  
26 distribution channels including, *inter alia*, its website and over the phone.

27 4. Delta provides air transportation for passengers in the United States and  
28 abroad. Delta offers its services through a system of hubs from Atlanta, Boston, Detroit,

1 Los Angeles, Minneapolis-St. Paul, New York, Salt Lake City, Seattle, and a number of  
2 international gateways. Delta sells tickets through various distribution channels including,  
3 *inter alia*, its website, mobile application, and over the phone.

4 5. In the last few years, retailers such as Target, Home Depot, Neiman Marcus,  
5 and Brooks Brothers have experienced streams of attacks on their data security.  
6 Implementing measures to prevent those attacks, as well as quickly identifying them, is a  
7 normal, expected part of the business—except in Defendants’ case.

8 6. On April 4, 2018, Delta acknowledged that customers using Delta’s online  
9 chat services, which were outsourced to 24/7, were subject to a data breach. In its  
10 statement, Delta stated its customers who used its customer support services during  
11 September and October of 2017 were potential victims of a breach in which their Customer  
12 Data was “exposed” and compromised (the “Data Breach”).<sup>1</sup> The Data Breach included  
13 payment information and other Customer Data.<sup>2</sup>

14 7. On April 5, 2018, Best Buy acknowledged that customers who used Best  
15 Buy’s outsourced chat services for customer support were similarly potential victims of the  
16 Data Breach and their Customer Data was stolen. Best Buy only acknowledged the Data  
17 Breach, however, after 24/7 informed Best Buy of the Data Breach, and after other  
18 companies—namely Delta and Sears—acknowledged the same Data Breach.<sup>3</sup>

19 8. This private Customer Data was compromised due to Best Buy’s and  
20 Delta’s, as well as their agent 24/7’s, acts and omissions and their failure to properly  
21 protect the Customer Data.

22 9. Defendants could have prevented this Data Breach. Data breaches in the last  
23 few years have been the result of infiltration of computer systems in which Customer Data  
24 is exchanged. While many retailers, restaurant chains, and other companies using such

25 <sup>1</sup> Delta, *Updated: Statement on [24]7.ai cyber incident*, <https://news.delta.com/updated-statement-247ai-cyber-incident> (last visited April 30, 2018).

26 <sup>2</sup> *Id.*; AP, *Delta says customers’ payment info breached in cyberattack*, <https://nypost.com/2018/04/04/delta-says-customers-payment-info-breached-in-cyberattack/> (last visited April 30, 2018).

27 <sup>3</sup> Brian Heater, *Best Buy Customer Info may have been Exposed in Data Breach*, TechCrunch,  
28 <https://techcrunch.com/2018/04/06/best-buy-customer-info-may-have-been-exposed-in-data-breach/> (last visited April 30, 2018).

1 systems have responded to recent breaches by adopting technology that helps make  
2 communication and transactions more secure, Defendants did not.

3 10. In addition to Defendants' failures to prevent the Data Breach, 24/7 also  
4 failed to disclose the Data Breach for approximately six (6) months, despite detecting and  
5 allegedly remedying the breach on October 12, 2017.<sup>4</sup>

6 11. The Data Breach was the inevitable result of Defendants' inadequate  
7 approach to data security and the protection of the Customer Data that it collected during  
8 the course of their business.

9 12. 24/7 acknowledges that it collects personal information, including: first and  
10 last names; organization names; email addresses; phone numbers; physical addresses; dates  
11 of birth; gender; professional title; account information; credit/debit card numbers; and  
12 other information 24/7 needs to provide client-specified services.<sup>5</sup> Indeed, 24/7 claims to  
13 follow "industry standards to protect the security of [users'] Personal Information and  
14 [24/7] respects [users'] choices for such information's intended use."<sup>6</sup> 24/7 allegedly uses  
15 "a combination of reasonable and appropriate physical, technical, and administrative  
16 safeguards to prevent unauthorized access or disclosure of [users'] Personal Information  
17 [... and] retains Personal Information and Interaction Data only as required or permitted by  
18 local law and while it has a legitimate business purpose."<sup>7</sup> Finally, 24/7 represents that it  
19 "uses standard security protocols, and mechanisms to exchange the transmission of  
20 sensitive Personal Information **such as credit card details and login credentials.**"<sup>8</sup>

21 13. Best Buy has recognized that:

22 Protecting customers' privacy is critical to Best Buy's growth  
23 and success. Customers entrust [Best Buy] with their personal  
24 information and it is [Best Buy's] responsibility to safeguard  
that data at all times. If Best Buy protects [its customers']

25 <sup>4</sup> *Id.*

26 <sup>5</sup> 24/7, Inc., Platform Privacy Policy, available at: <https://www.247.ai/privacy-policy#platform-policy> (last  
visited April 30, 2018).

27 <sup>6</sup> *Id.*

28 <sup>7</sup> *Id.*

<sup>8</sup> *Id.*

1 personal information, customers are more likely to become,  
2 and remain, loyal to [Best Buy's] brand. If this trust is broken,  
3 Best Buy risks negative publicity, fines and lawsuits, lost sales,  
4 and damage to [Best Buy's] business and reputation.”<sup>9</sup>

5 14. Delta acknowledges that “Information Security is important to Delta,” and:

6 [Delta has] established appropriate physical, electronic and  
7 managerial safeguards to protect the information we collect  
8 from or about our users. These safeguards are regularly  
9 reviewed to protect against unauthorized access, disclosure and  
10 improper use of your information, and to maintain the accuracy  
11 and integrity of that data.<sup>10</sup>

12 15. Delta further acknowledges that it collects: names, address, and telephone  
13 numbers; dates of birth; gender; redress numbers; known traveler numbers; email  
14 addresses; cell phone numbers; credit and debit card numbers, associated billing addresses,  
15 and expiration dates; emergency contacts, medical needs, and dietary requests; and other  
16 personal identifiable information.<sup>11</sup> Delta last updated this privacy policy on January 7,  
17 2013.<sup>12</sup>

18 16. Delta further informs customers that it may engage third parties to process  
19 information and assist in improving the customer service experience, but “requires that  
20 these third parties comply with Delta’s Privacy Policy” when processing customers’ private  
21 and sensitive Customer Data.<sup>13</sup>

22 17. Unfortunately, Defendants, did not hold true to their security promises,  
23 despite any efforts to place the ultimate onus on consumers.

24 18. Instead, Defendants disregarded the rights of Plaintiffs and the Class and  
25 Subclass members, by, through themselves and their agent 24/7, intentionally, willfully,  
26 recklessly, or negligently failing to take adequate and reasonable measures to ensure  
27 Defendants’ data systems were protected, failing to disclose to their customers the material

28 <sup>9</sup> Best Buy Code of Business Ethics, Privacy Policy, *available at*:  
<https://secure.ethicspoint.com/domain/media/en/gui/26171/code.html?section=7&sub=4> (last visited April 30,  
2018).

<sup>10</sup> Delta, Cookies, Privacy & Security, *available at*: [https://www.delta.com/content/www/en\\_US/privacy-and-security.html](https://www.delta.com/content/www/en_US/privacy-and-security.html) (last visited April 30, 2018)

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

1 fact that they did not have adequate computer systems and security practices to safeguard  
2 Customer Data, failing to take available steps to prevent and stop the breach from ever  
3 happening, failing to timely monitor and detect the Data Breach, and failing to timely  
4 notify consumers of the Data Breach.

5 19. In addition, 24/7, as the agent of Best Buy and Delta, exacerbated the  
6 damages Plaintiffs and the Class and Subclass members suffered by failing to timely detect  
7 the infiltration and failing to timely notify customers their Customer Data had been  
8 compromised. If 24/7 had detected the malware earlier and promptly notified Best Buy,  
9 Delta, and the public of the Data Breach, the resulting losses would have been far less  
10 significant.

11 20. As a result of Defendants' Data Breach, the Customer Data of Plaintiffs and  
12 the Class and Subclass members has been exposed to criminals for misuse, the obvious  
13 reason for which this information was taken . The damages Plaintiffs and the Class and  
14 Subclass members suffered as a direct result of the Data Breach include:

- 15 a. unauthorized charges on their debit and credit card accounts;
- 16 b. theft of their personal and financial information;
- 17 c. costs associated with the detection and prevention of identity theft and  
18 unauthorized use of their financial accounts;
- 19 d. damages arising from the inability to use their debit or credit card  
20 accounts because their account were suspended or otherwise rendered  
21 unusable as a result of fraudulent charges stemming from the Data  
22 Breach;
- 23 e. loss of use of and access to their account funds and costs associated with  
24 inability to obtain money from their accounts or being limited in the  
25 amount of money they were permitted to obtain from their accounts,  
26 including missed payments on bills and loans, late charges and fees, and  
27 adverse effects on their credit including decreased credit scores and  
28 adverse credit notations;

1 f. costs associated with time spent and the loss of productivity or the  
2 enjoyment of one's life from taking time to address and attempt to  
3 ameliorate, mitigate and deal with the actual and future consequences of  
4 the Data Breach, including finding fraudulent charges, cancelling and  
5 reissuing cards, purchasing credit monitoring and identity theft  
6 protection services, imposition of withdrawal and purchase limits on  
7 compromised accounts, and the stress, nuisance and annoyance of  
8 dealing with all issues resulting from the Data Breach;

9 g. the imminent and certainly impending injury flowing from potential  
10 fraud and identity theft posed by their credit card and personal  
11 information being placed in the hands of criminals and already misused  
12 via the sale of Plaintiffs' and the Class and Subclass members'  
13 information on the Internet black market;

14 h. money paid for merchandise purchased at Best Buy stores during the  
15 period of the Data Breach, in that Plaintiff and the Class and Subclass  
16 members would not have shopped at Best Buy had Defendants disclosed  
17 that they lacked adequate systems and procedures to reasonably  
18 safeguard customers' Customer Data, or Plaintiff and the Class and  
19 Subclass members would have taken measures to protect their Customer  
20 Data had Defendants made such disclosures;

21 i. damages to and diminution in value of their Customer Data entrusted to  
22 Defendants for the sole purpose of purchasing merchandise from Best  
23 Buy; and

24 j. the loss of Plaintiffs' and the Class and Subclass members' privacy.

25 21. The damages to Plaintiffs and the Class and Subclass members were  
26 directly and proximately caused by Defendants' failure to implement or maintain adequate  
27 data security measures for Customer Data.

28 22. The damages to Plaintiffs and the Class and Subclass members were also

1 directly and proximately caused by Defendants' failure to inform customers that their  
2 Customer Data was subject to collection and storage by the outsourced customer service  
3 corporation 24/7.

4 23. Further, Plaintiffs retain a significant interest in ensuring that their  
5 Customer Data, which, while stolen, remains in the possession of Defendants, is protected  
6 from further breaches, and seek to remedy the harms they have suffered on behalf of  
7 themselves and other similarly situated consumers whose Customer Data was stolen as a  
8 result of the Data Breach.

9 24. Plaintiffs, on behalf of themselves and other similarly situated consumers,  
10 seek to recover damages, equitable relief including injunctive relief to prevent a  
11 reoccurrence of the Data Breach and resulting injury, restitution, disgorgement, reasonable  
12 costs and attorneys' fees, and all other remedies this Court deems proper.

13 **JURISDICTION AND VENUE**

14 25. This Court has subject matter jurisdiction over this action pursuant to the  
15 Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount  
16 in controversy exceeds \$5,000,000, exclusive of interests and costs, there are more than  
17 100 class members, and at least one class member is a citizen of a state different from  
18 Defendants.

19 26. This Court has personal jurisdiction over 24/7 because 24/7: 1) is  
20 headquartered in this District; 2) conducts substantial business in the District; and 3)  
21 committed the acts and omissions complained of in the District.

22 27. This Court has personal jurisdiction over Best Buy because Best Buy: 1)  
23 conducts substantial business in this District; and 2) committed the acts and omissions  
24 complained of in this District.

25 28. This Court has personal jurisdiction over Delta because Delta: 1) conducts  
26 substantial business in this District; and 2) committed the acts and omissions complained of  
27 in this District.



1           37.     The compromise of the Best Buy Plaintiff's payment card occurred even  
2 though he had physical possession of the card at all times. He was required to expend time  
3 communicating with the card issuer attempting to resolve the issues caused by the theft of  
4 his credit card and other personal information used to accomplish the fraudulent activity.

5           38.     The Best Buy Plaintiff would not have used his payment card, Best Buy's  
6 online store, and Best Buy's agent 24/7's customer service client to make purchases at and  
7 communicate with Best Buy had 24/7 and Best Buy told him they lacked adequate  
8 computer systems and data security practices to safeguard customers' Customer Data from  
9 theft. Indeed, the Best Buy Plaintiff would not have shopped at Best Buy at all during the  
10 period of the Data Breach and, thus, he suffered actual injury and damages in paying  
11 money for the purchase of merchandise from Best Buy that he would not have paid had  
12 24/7 and Best Buy made such disclosures.

13           39.     The Best Buy Plaintiff suffered actual injury from having his Customer Data  
14 compromised and stolen in and as a result of the Data Breach.

15           40.     The Best Buy Plaintiff also suffered actual injury in the form of damages to  
16 and diminution in the value of his Customer Data—a form of intangible property that he  
17 entrusted to Best Buy and its agent 24/7 as a form of payment for merchandise and that was  
18 compromised in and as a result of the Data Breach.

19           41.     The Best Buy Plaintiff further suffered actual injury in the form of time  
20 spent dealing with fraud resulting from the Data Breach, disputing the fraudulent charges,  
21 and monitoring his account for additional fraud.

22           42.     Additionally, the Best Buy Plaintiff has suffered imminent and impending  
23 injury arising from the substantially increased risk of future fraud, identity theft, and  
24 misuse posed by his Customer Data being placed in the hands of criminals who have  
25 already misused such information, as evidenced by the compromise of his payment card.

26           43.     Moreover, the Best Buy Plaintiff has a continuing interest in ensuring that  
27 his private information, which remains in the possession of 24/7 and Best Buy, is protected  
28 and safeguarded from future breaches.

1 **B. The Delta Plaintiff's Transactions**

2 44. The Delta Plaintiff makes purchases with Delta through Delta's mobile  
3 application and website, and uses the online chat function to communicate with customer  
4 service. For his purchases, he uses a credit card.

5 45. Recently, the Delta Plaintiff reviewed his financial statements and identified  
6 numerous transactions that were determined to be fraudulent activity. Due to this fraudulent  
7 activity, he changed his passwords and signed up for fraud protection services.

8 46. The compromise of the Delta Plaintiff's payment card occurred even though  
9 he had physical possession of the card at all times. He was required to expend time  
10 communicating with the card issuer attempting to resolve the issues caused by the theft of  
11 his credit card and other personal information used to accomplish the fraudulent activity.

12 47. The Delta Plaintiff would not have used his payment card, Delta's website  
13 and mobile app, and Delta's agent 24/7's customer service client to make Delta purchases  
14 and communicate with Delta had 24/7 and Delta told him they lacked adequate computer  
15 systems and data security practices to safeguard customers' Customer Data from theft.  
16 Indeed, the Delta Plaintiff would not have patronized Delta at all during the period of the  
17 Data Breach and, thus, he suffered actual injury and damages in paying money for the  
18 purchase of air travel from Delta that he would not have paid had 24/7 and Delta made such  
19 disclosures.

20 48. The Delta Plaintiff suffered actual injury from having his Customer Data  
21 compromised and stolen in and as a result of the Data Breach.

22 49. The Delta Plaintiff also suffered actual injury in the form of damages to and  
23 diminution in the value of his Customer Data—a form of intangible property that he  
24 entrusted to Delta and its agent 24/7 as a form of payment for merchandise and that was  
25 compromised in and as a result of the Data Breach.

26 50. The Delta Plaintiff further suffered actual injury in the form of time spent  
27 dealing with fraud resulting from the Data Breach, disputing the fraudulent charges,  
28 signing up for third-party monitoring, and monitoring his account for additional fraud.

1           51.     Additionally, the Delta Plaintiff has suffered imminent and impending  
2 injury arising from the substantially increased risk of future fraud, identity theft, and  
3 misuse posed by his Customer Data being placed in the hands of criminals who have  
4 already misused such information, as evidenced by the compromise of his payment card.

5           52.     Moreover, the Delta Plaintiff has a continuing interest in ensuring that his  
6 private information, which remains in the possession of 24/7 and Delta, is protected and  
7 safeguarded from future breaches.

### 8     **C.     Defendants Collect and Store PII for their Own Financial Gain**

9           53.     Founded in 2000,<sup>14</sup> 24/7 operates a variety of customer services products  
10 with artificial intelligence technologies with additional offices in Toronto, London,  
11 Stockholm, and Sydney, and numerous clients in retail, education, financial services,  
12 healthcare, insurance, travel and hospitality, and utilities.<sup>15</sup>

13           54.     Since its founding, 24/7 has aggressively expanded, including private  
14 funding from Sequoia Capital—a venture capital firm controlling \$1.4 trillion in assets—in  
15 2003, as well as a partnership with Microsoft in 2012, in which Microsoft combined its  
16 “interactive self-service assets” with 24/7’s technologies.<sup>16</sup>

17           55.     At all relevant times, Defendants were well-aware, or reasonably should  
18 have been aware, that the Customer Data collected, maintained, and stored in their agent  
19 24/7’s computer systems is highly sensitive, susceptible to attack, and could be used for  
20 wrongful purposes by third parties, such as identity theft and fraud.

21           56.     It is well known and the subject of many media reports that Customer Data  
22 is highly coveted and a frequent target of hackers. Despite the frequent public  
23 announcements of data breaches by other retailers, Defendants maintained an insufficient  
24 and inadequate system to protect Plaintiff’s and the Class and Subclass members’

25 \_\_\_\_\_  
26 <sup>14</sup> [24]7 Company Profile, Forbes, <https://www.forbes.com/companies/24-7/> (last visited April 30, 2018);

27 <sup>15</sup> [24]7 Company Overview, <https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapid=4532786> (last visited April 30, 2018)

28 <sup>16</sup> *Microsoft picks stake in Sequoia-backed 24/7 Inc*, Reuters, <https://in.reuters.com/article/microsoft-picks-stake-in-sequoia-backed-idINDEE81807U20120209> (last visited May 1, 2018)

1 Customer Data.

2 57. Customer Data is a valuable commodity because it contains not only  
3 payment card numbers but PII as well. A “cyber blackmarket” exists in which criminals  
4 openly post stolen payment card numbers, and other personal information on a number of  
5 underground Internet websites. Customer Data is “as good as gold” to identity thieves  
6 because they can use victims’ personal data to open new financial accounts and take out  
7 loans in another person’s name, incur charges on existing accounts, or clone ATM, debit,  
8 or credit cards.

9 58. Legitimate organizations and the criminal underground alike recognize the  
10 value in PII contained in a merchant’s data systems; otherwise, they would not aggressively  
11 seek or pay for it. For example, in “one of 2013’s largest breaches . . . not only did hackers  
12 compromise the [card holder data] of three million customers, they also took registration  
13 data [containing PII] from 38 million users.”<sup>17</sup>

14 59. At all relevant times, Defendants knew, or reasonably should have known,  
15 of the importance of safeguarding Customer Data and of the foreseeable consequences that  
16 would occur if Defendants’, and particular 24/7’s (as an agent of each Defendant), data  
17 security systems were breached, including, specifically, the significant costs that would be  
18 imposed on their customers as a result of a data breach.

19 60. Defendants were, or reasonably should have been, fully aware of the  
20 significant volume of daily credit and debit card transactions and PII provided in customer  
21 service interactions and purchase and, thus, the significant number of individuals who  
22 would be harmed by a breach of Defendants’ systems.

23 61. Unfortunately, and as alleged below, despite all of this publicly available  
24 knowledge of the continued compromises of Customer Data in the hands of other third  
25 parties, such as retailers, Defendants’ approach to maintaining the privacy and security  
26

27 <sup>17</sup> Verizon 2014 PCI Compliance Report, available at:  
28 [http://www.cisco.com/c/dam/en\\_us/solutions/industries/docs/retail/verizon\\_pci2014.pdf](http://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/verizon_pci2014.pdf) (hereafter “2014  
Verizon Report”), at 54 (last visited April 30, 2018).

1 Plaintiffs' and the Class and Subclass members' Customer Data was lackadaisical, cavalier,  
2 reckless, or at the very least, negligent.

3 **D. Defendants Had Notice of Data Breaches Involving Malware on POS Systems**

4 62. A wave of data breaches causing the theft of retail payment card information  
5 has hit the United States in the last several years.<sup>18</sup> In 2016, the number of U.S. data  
6 breaches surpassed 1,000, a record high and a forty percent increase in the number of data  
7 breaches from the previous year.<sup>19</sup> The amount of payment card data compromised by data  
8 breaches is massive. For example, it is estimated that over 100 million cards were  
9 compromised in 2013 and 2014.<sup>20</sup>

10 63. Most of the massive data breaches occurring within the last several years  
11 involved malware placed on computer systems that retail merchants and their agents use.

12 64. These massive data breaches involve compromising payment systems at  
13 physical retail outlets, phishing schemes to gain access to internal servers and information,  
14 as well as exploiting other vulnerabilities in companies' websites and electronically stored  
15 data systems.

16 **E. Defendants' Data Breach**

17 65. On April 4, 2018, Delta announced the Data Breach, and on April 5, 2018,  
18 Best Buy followed. According to their respective statements, Best Buy and Delta were  
19 informed of the Data Breach on March 28, 2018.

20 66. 24/7 possibly knew of the Data Breach as early as September 26, 2017, and  
21 definitively on October 12, 2017, when 24/7 allegedly fixed the security issues.<sup>21</sup>

22  
23  
24 <sup>18</sup> *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and*  
25 *CyberScout*, Identity Theft Resource Center (Jan. 19, 2017), <http://www.prnewswire.com/news-releases/data-breaches-increase-40-percent-in-2016-finds-new-report-from-identity-theft-resource-center-and-cyberscout-300393208> (last visited April 13, 2018).

26 <sup>19</sup> *Id.*

27 <sup>20</sup> Symantec, *A Special Report On Attacks On Point-of-Sale Systems*, p. 3 (Nov. 20, 2014), available at:  
28 <https://origin-www.symantec.com/content/dam/symantec/docs/white-papers/attacks-on-point-of-sale-systems-en.pdf> (last visited April 13, 2018).

<sup>21</sup>

1           67. Despite knowing of the Data Breach as of October 12, 2017—over six (6)  
2 months ago—24/7 has not provided much-if-any details regarding the degree and extent of  
3 the Data Breach, despite handling chat services for Best Buy, Delta, Sears, and a number of  
4 other companies.

5           **F. The Data Breach Caused Harm and Will Result in Additional Fraud**

6           68. Without detailed disclosure of the nature and scope of the Data Breach,  
7 consumers, including Plaintiffs and the Class and Subclass members, have been left  
8 exposed—unknowingly and unwittingly—for months to continued misuse and ongoing risk  
9 of misuse of their personal information without being able to take necessary precautions to  
10 prevent imminent harm.

11           69. The ramifications of Defendants’ failure to keep Plaintiffs’ and the Class  
12 and Subclass members’ Costumer Data secure are severe.

13           70. The FTC defines identity theft as “a fraud committed or attempted using the  
14 identifying information of another person without authority.”<sup>22</sup> The FTC describes  
15 “identifying information” as “any name or number that may be used, alone or in  
16 conjunction with any other information, to identify a specific person.”<sup>23</sup>

17           71. Personal identifying information is a valuable commodity to identity thieves  
18 once the information has been compromised. As the FTC recognizes, once identity thieves  
19 have personal information, “they can drain your bank account, run up your credit cards,  
20 open new utility accounts, or get medical treatment on your health insurance.”<sup>24</sup>

21           72. Identity thieves can use personal information, such as Plaintiffs’ and the  
22 Class and Subclass members’, which Defendants failed to keep secure, to perpetrate a  
23 variety of crimes that harm victims. For instance, identity thieves may commit various  
24 types of government fraud such as: immigration fraud; obtaining a driver’s license or  
25 identification card in the victim’s name but with another’s picture; using the victim’s

26 \_\_\_\_\_  
27 <sup>22</sup> 17 C.F.R. § 248.201 (2013).

<sup>23</sup> *Id.*

28 <sup>24</sup> Federal Trade Commission, *Warning Signs of Identity Theft*, available at:  
<https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft> (last visited April 13, 2018).

1 information to obtain government benefits; or filing a fraudulent tax return using the  
2 victim's information to obtain a fraudulent refund.

3 73. Javelin Strategy and Research reports that identity thieves have stolen \$112  
4 billion in the past six years.<sup>25</sup>

5 74. Reimbursing a consumer for a financial loss due to fraud does not make that  
6 individual whole again. On the contrary, identity theft victims must spend numerous hours  
7 and their own money repairing the impact to their credit. After conducting a study, the  
8 Department of Justice's Bureau of Justice Statistics ("BJS") found that identity theft  
9 victims "reported spending an average of about 7 hours clearing up the issues" and  
10 resolving the consequences of fraud in 2014.<sup>26</sup>

11 75. There may be a time lag between when harm occurs versus when it is  
12 discovered, and also between when PII or PCD is stolen and when it is used. According to  
13 the U.S. Government Accountability Office ("GAO"), which conducted a study regarding  
14 data breaches:

15 [L]aw enforcement officials told us that in some cases, stolen  
16 data may be held for up to a year or more before being used to  
17 commit identity theft. Further, once stolen data have been sold  
18 or posted on the Web, fraudulent use of that information may  
19 continue for years. As a result, studies that attempt to measure  
20 the harm resulting from data breaches cannot necessarily rule  
21 out all future harm.<sup>27</sup>

22 76. Plaintiffs and the Class and Subclass members now face years of constant  
23 surveillance of their financial and personal records, monitoring, and loss of rights.  
24 Plaintiffs and the Class and Subclass members are incurring and will continue to incur  
25 such damages in addition to any fraudulent credit and debit card charges incurred by them

26 <sup>25</sup> See <https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point> (last  
visited April 13, 2018).

27 <sup>26</sup> Victims of Identity Theft, 2014 (Sept. 2015) available at: <http://www.bjs.gov/content/pub/pdf/vit14.pdf> (last  
visited April 13, 2018).

28 <sup>27</sup> GAO, Report to Congressional Requesters, at 29 (June 2007), available at  
<http://www.gao.gov/new.items/d07737.pdf> (last visited April 13, 2018).

1 and the resulting loss of use of their credit and access to funds, whether or not such  
2 charges are ultimately reimbursed by the credit card companies.

3 **G. Plaintiffs and the Class and Subclass Members Suffered Damages**

4 77. Plaintiffs' and the Class and Subclass members' Customer Data is private  
5 and sensitive in nature, and Defendants left that Customer Data inadequately protected.  
6 Defendants did not obtain Plaintiffs' and the Class and Subclass members' consent to  
7 disclose their Customer Data to any other person as required by applicable law and industry  
8 standards.

9 78. The Data Breach was a direct and proximate result of Defendants' failure to  
10 properly safeguard and protect Plaintiffs' and the Class and Subclass members' Customer  
11 Data from unauthorized access, use, and disclosure, as required by various state and federal  
12 regulations, industry practices, and the common law, including Defendants' failure to  
13 establish and implement appropriate administrative, technical, and physical safeguards to  
14 ensure the security and confidentiality of Plaintiffs' and the Class and Subclass members'  
15 Customer Data to protect against reasonably foreseeable threats to the security or integrity  
16 of such information.

17 79. Defendants had the resources to prevent a breach, especially with the  
18 partnerships with Sequoia Capital and Microsoft.

19 80. Had Defendants employed security measures recommended by experts in  
20 the field, Defendants would have prevented intrusion into their computer systems and,  
21 ultimately, the theft of their customers' Customer Data.

22 81. As a direct and proximate result of Defendants' wrongful actions and  
23 inaction and the resulting Data Breach, Plaintiffs and the Class and Subclass members  
24 have been placed at an imminent, immediate, and continuing increased risk of harm from  
25 identity theft and identity fraud, requiring them to take the time which they otherwise  
26 would have dedicated to other life demands such as work and effort to mitigate the actual  
27 and potential impact of the Data Breach on their lives including, *inter alia*, by placing  
28 "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions,

1 closing or modifying financial accounts, closely reviewing and monitoring their credit  
2 reports and accounts for unauthorized activity, and filing police reports. This time has been  
3 lost forever and cannot be recaptured. In all manners of life in this country, time has  
4 constantly been recognized as compensable, for many consumers it is the way they are  
5 compensated, and even if retired from the work force, consumers should be free of having  
6 to deal with the consequences of a retailer's slippage, as is the case here.

7 82. Defendants' wrongful actions and inaction directly and proximately caused  
8 the theft and dissemination into the public domain of Plaintiffs' and the Class and  
9 Subclass members' Customer Data, causing them to suffer, and continue to suffer,  
10 economic damages and other actual harm for which they are entitled to compensation,  
11 including:

- 12 a. theft of their personal and financial information;
- 13 b. unauthorized charges on their debit and credit card accounts;
- 14 c. the imminent and certainly impending injury flowing from potential  
15 fraud and identity theft posed by their credit/debit card and personal  
16 information being placed in the hands of criminals and already misused  
17 via the sale of Plaintiffs' and the Class and Subclass members'  
18 information on the Internet black market;
- 19 d. the untimely and inadequate notification of the Data Breach;
- 20 e. the improper disclosure of their Customer Data;
- 21 f. loss of privacy;
- 22 g. the monetary amount of purchases at Best Buy and Delta during the  
23 period of the Data Breach in that Plaintiffs and the Class and Subclass  
24 members would not have patronized Best Buy and Delta, or at least  
25 would not have used their payment cards for online purchases, had  
26 Defendants disclosed that Defendants lacked adequate systems and  
27 procedures to reasonably safeguard customers' financial and personal  
28

1 information and had Defendants provided timely and accurate notice of  
2 the Data Breach;

3 h. ascertainable losses in the form of out-of-pocket expenses and the value  
4 of their time reasonably incurred to remedy or mitigate the effects of the  
5 Data Breach;

6 i. ascertainable losses in the form of deprivation of the value of their PII  
7 and PCD, for which there is a well-established national and international  
8 market;

9 j. ascertainable losses in the form of the loss of cash back or other benefits  
10 as a result of their inability to use certain accounts and cards affected by  
11 the Data Breach;

12 k. loss of use of and access to their account funds and costs associated with  
13 the inability to obtain money from their accounts or being limited in the  
14 amount of money they were permitted to obtain from their accounts,  
15 including missed payments on bills and loans, late charges and fees, and  
16 adverse effects on their credit including adverse credit notations; and,

17 l. the loss of productivity and value of their time spent to address attempt  
18 to ameliorate, mitigate and deal with the actual and future consequences  
19 of the data breach, including finding fraudulent charges, cancelling and  
20 reissuing cards, purchasing credit monitoring and identity theft  
21 protection services, imposition of withdrawal and purchase limits on  
22 compromised accounts, and the stress, nuisance and annoyance of  
23 dealing with all such issues resulting from the Data Breach.

24 83. Best Buy and Delta—but not 24/7—have stated that affected  
25 customers will be offered credit monitoring or identity theft protection services,  
26 but have not come forth with any details as to how to sign up, the type of  
27 coverage, the scope of coverage, or the length of coverage. As a result, Plaintiffs  
28 and the Class and Subclass members are left to their own actions to protect

1 themselves from the financial damage Defendants have allowed to occur. The  
2 additional cost of adequate and appropriate coverage, or insurance, against the  
3 losses and exposure that Defendants' actions have created for Plaintiffs and the  
4 Class and Subclass members is ascertainable and is a determination appropriate  
5 for the trier of fact.

6 84. While Plaintiffs' and the Class and Subclass members' Customer  
7 Data has been stolen, Defendants continue to hold Customer Data of consumers,  
8 including Plaintiffs, the Class members, and the subclass members. Particularly  
9 because Defendants have demonstrated an inability to prevent a breach or stop it  
10 from continuing even after being detected, Plaintiffs and the Class and Subclass  
11 members have an undeniable interest in ensuring that their Customer Data is  
12 secure, remains secure, is properly and promptly destroyed, and is not subject to  
13 further theft.

#### 14 **CHOICE OF LAW**

15 85. California, which seeks to protect the rights and interests of California and  
16 other U.S. residents against a company doing business in California, has a greater interest  
17 in the claims of Plaintiffs and the Class and Subclass members than any other state and is  
18 most intimately concerned with the claims and outcome of this litigation.

19 86. The principal place of business of 24/7—which both Best Buy and Delta  
20 entrusted to provide services as their agent—is located at 910 East Hamilton Avenue, Suite  
21 240, Campbell, CA 95008, is the “nerve center” of 24/7's business activities—the place  
22 where high-level officers direct, control, and coordinate 24/7's activities, including data  
23 security, and where: a) major policy; b) advertising; c) distribution; d) accounts receivable  
24 departments; and e) financial and legal decisions originate.

25 87. Data security assessments and other IT duties related to computer systems  
26 and data security occur at 24/7's California headquarters.

27 88. Furthermore, 24/7's response, and corporate decisions surrounding such  
28 response, to the Data Breach were made from and in California.

1 89. 24/7's breach of their duty to customers—including Plaintiff and the Class  
2 and Subclass members—emanated from California.

3 90. Moreover, because 24/7 is headquartered in California and its key decisions  
4 and operations emanate from California, California law can and should apply to claims  
5 relating to the Data Breach, even those made by persons who reside outside of California.  
6 In fact, California law should apply to all of Plaintiffs' claims, as Best Buy and Delta  
7 entrusted 24/7 to handle and make decisions, and 24/7's substandard acts happened in  
8 California, and, upon information and belief, the Plaintiff's PII was collected, stored on,  
9 and routed through California-, and United States-based servers. For the sake of fairness  
10 and efficiency, California law should apply to these claims.

11 91. Application of California law to a nationwide Class with respect to  
12 Plaintiffs' and the Class and Subclass members' claims is neither arbitrary nor  
13 fundamentally unfair because California has significant contacts and a significant  
14 aggregation of contacts that create a state interest in the claims of the Plaintiffs, the  
15 nationwide Class, and the respective subclasses.

16 92. Further, under California's choice of law principles, which are applicable to  
17 this action, the common law of California will apply to the common law claims of all Class  
18 members.

### 19 CLASS ACTION ALLEGATIONS

20 93. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil  
21 Procedure, Plaintiffs bring this lawsuit on behalf of themselves and as a class action on  
22 behalf of the following classes of individuals:

23	NATIONWIDE CLASS:	All persons who used 24/7's electronic customer
24	(or the CLASS)	service platform and whose Customer Data was
25	BEST BUY SUBCLASS:	compromised as a result of the Data Breach.
26		All consumers who used Best Buy's
27		electronic customer service platform and whose
28		Customer Data was compromised as a result of
		the Data Breach.
	DELTA SUBCLASS:	All consumers who used Delta's electronic

customer service platform and whose Customer Data was compromised as a result of the Data Breach.

1  
2  
3 94. Excluded from the Class are Defendants and any entities in which any  
4 Defendant or their subsidiaries or affiliates have a controlling interest; Defendants'  
5 officers, agents, and employees; and all persons who make a timely election to be excluded  
6 from the Nationwide Class and any subclasses. Also excluded from the Class are the judge  
7 assigned to this action, and any member of the judge's immediate family.

8 95. **Numerosity:** The members of each Class are so numerous that joinder of all  
9 members of any Class would be impracticable. Plaintiffs reasonably believe that the  
10 Nationwide Class members number in the hundreds of thousands of people or more in the  
11 aggregate, and well over 1,000 in the smallest of the classes. Similarly, Plaintiffs  
12 reasonably believe that the Best Buy and Delta Subclass members number in the hundreds  
13 of thousands of people or more in the aggregate, and well over 1,000 in the smallest of  
14 classes. The names and addresses of the Class and Subclass members are identifiable  
15 through documents Defendants maintain.

16 96. **Commonality and Predominance:** This action involves common questions  
17 of law or fact, which predominate over any questions affecting individual Class and  
18 Subclass members, including:

- 19 i. Whether Defendants owed a legal duty to Plaintiffs and the Class and  
20 Subclass members to exercise due care in collecting, storing, and  
21 safeguarding their Customer Data;
- 22 ii. Whether Defendants breached a legal duty to Plaintiffs and the Class  
23 and Subclass members to exercise due care in collecting, storing, and  
24 safeguarding their Customer Data;
- 25 iii. Whether Defendants knew or should have known of the susceptibility  
26 of their computer systems to a data breach;
- 27 iv. Whether Defendants' security measures to protect their computer  
28 systems were reasonable in light of industry data security

1 recommendations, and other measures data security experts  
2 recommended;

3 v. Whether Defendants willfully, recklessly, or negligently failed to  
4 maintain and execute reasonable procedures designed to prevent  
5 unauthorized access to Plaintiffs' and the Class and Subclass  
6 members' Customer Data;

7 vi. Whether Plaintiffs' and the Class and Subclass members' Customer  
8 Data was accessed, exposed, compromised, or stolen in the Data  
9 Breach;

10 vii. Whether Defendants were negligent in failing to implement reasonable  
11 and adequate security procedures and practices;

12 viii. Whether Defendants' failure to implement adequate data security  
13 measures allowed the breach of their computer systems to occur;

14 ix. Whether Defendants' conduct constituted deceptive trade practices  
15 under California law;

16 x. Whether Defendants' conduct, including their failure to act, resulted in  
17 or was the proximate cause of the breach of their systems, resulting in  
18 the loss of Plaintiffs' and the Class and Subclass members' Customer  
19 Data;

20 xi. Whether Defendants failed to timely notify the public of the Data  
21 Breach;

22 xii. Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;

23 xiii. Whether Defendants' conduct was an unlawful or unfair business  
24 practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;

25 xiv. Whether Defendants' conduct violated § 5 of the Federal Trade  
26 Commission Act, 15 U.S.C. § 45, *et seq.*;

1           xv.       Whether Plaintiffs and the Class and Subclass members are entitled to  
2                   equitable relief, including, but not limited to, injunctive relief and  
3                   restitution; and

4           xvi.       Whether Plaintiffs and the Class and Subclass members are entitled to  
5                   actual, statutory, or other forms of damages, and other monetary relief.

6           97.       Defendants engaged in a common course of conduct giving rise to the legal  
7                   rights sought to be enforced by Plaintiff individually and on behalf of the Class and  
8                   Subclass members. Similar or identical statutory and common law violations, business  
9                   practices, and injuries are involved. Individual questions, if any, pale by comparison, in  
10                  both quantity and quality, to the numerous common questions that dominate this action.

11           98.       **Typicality:** Plaintiffs' claims are typical of the Class and Subclass  
12                   members' claims because, among other things, Plaintiffs and the Class and Subclass  
13                   members were injured through Defendants' substantially uniform misconduct. Plaintiffs are  
14                   advancing the same claims and legal theories on behalf of themselves and the Class and  
15                   Subclass members, and there are no defenses that are unique to Plaintiffs' claims.  
16                   Plaintiffs' and the Class and Subclass members' claims arise from the same operative facts  
17                   and are based on the same legal theories.

18           99.       **Adequacy of Representation:** Plaintiffs are adequate representatives of the  
19                   Nationwide Class and the respective subclasses because their interests do not conflict with  
20                   the interests of the other class and subclass members they seek to represent; Plaintiffs have  
21                   retained counsel competent and experienced in complex class action litigation; and  
22                   Plaintiffs will prosecute this action vigorously. The Class and subclass members' interests  
23                   will be fairly and adequately protected by Plaintiffs and their counsel.

24           100.       **Superiority:** A class action is superior to any other available means for the  
25                   fair and efficient adjudication of this controversy, and no unusual difficulties are likely to  
26                   be encountered in the management of this matter as a class action. The damages, harm, or  
27                   other financial detriment suffered individually by Plaintiffs and the Class and Subclass  
28                   members are relatively small compared to the burden and expense that would be required

1 to litigate their claims on an individual basis against Defendants, making it impracticable  
2 for the Class and Subclass members to individually seek redress for Defendants' wrongful  
3 conduct. Even if the Class and Subclass members could afford individual litigation, the  
4 court system could not. Individualized litigation would create a potential for inconsistent or  
5 contradictory judgments and increase the delay and expense to all parties and the court  
6 system. By contrast, the class action device presents far fewer management difficulties and  
7 provides the benefits of single adjudication, economies of scale, and comprehensive  
8 supervision by a single court.

9 101. Further, Defendants have acted or refused to act on grounds generally  
10 applicable to the Class and Subclass and, accordingly, final injunctive or corresponding  
11 declaratory relief with regard to the members of the Class as a whole is appropriate under  
12 Rule 23(b)(2) of the Federal Rules of Civil Procedure.

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

- 17 a. Whether the Class and Subclass members' Customer Data was  
18 accessed, exposed, compromised, or stolen in the Data Breach;
- 19 b. Whether (and when) Defendants knew about the Data Breach before it  
20 was announced to the public and whether Defendants failed to timely  
21 notify the public of the Data Breach;
- 22 c. Whether Defendants misrepresented the safety of their many systems  
23 and services, specifically the security thereof, and their ability to safely  
24 store Plaintiffs and the Class and Subclass members' Customer Data;
- 25 d. Whether Defendants concealed crucial information about their  
26 inadequate data security measures from Plaintiffs and the Class and  
27 Subclass members;

- 1 e. Whether Defendants failed to comply with their own policies and  
2 applicable laws, regulations, and industry standards relating to data  
3 security;
- 4 f. Whether Defendants' acts, omissions, misrepresentations, and  
5 practices were and are likely to deceive consumers;
- 6 g. Whether Defendants knew or should have known that they did not  
7 employ reasonable measures to keep Plaintiffs' and the Class and  
8 Subclass members' Customer Data secure and prevent the loss or  
9 misuse of that information;
- 10 h. Whether Defendants failed to implement and maintain reasonable  
11 security procedures and practices for Plaintiffs' and the Class and  
12 Subclass members' Customer Data in violation of Section 5 of the  
13 FTC Act;
- 14 i. Whether Defendants failed to provide timely notice of the Data  
15 Breach, to Plaintiff and the Class and Subclass members;
- 16 j. Whether Defendants conduct violated Cal. Bus. & Prof. Code § 22575,  
17 *et seq.*;
- 18 k. Whether Defendants owed a duty to Plaintiffs and the Class and  
19 Subclass members to safeguard their Customer Data and to implement  
20 adequate data security measures;
- 21 l. Whether Defendants failed to adhere to their posted privacy policies  
22 concerning the care they would take to safeguard Plaintiffs' and the  
23 Class and Subclass members' Customer Data in violation of Cal. Bus.  
24 & Prof. Code § 22576;
- 25 m. Whether Defendants negligently and materially failed to adhere to  
26 their posted privacy policies concerning the safeguarding of Plaintiffs'  
27 and the Class and Subclass members' Customer Data in violation of  
28 Cal. Bus. & Prof. Code § 22576;

- 1 n. Whether Defendants breached that duty;
- 2 o. Whether an implied contract existed between Defendants and Plaintiffs
- 3 and the Class and Subclass members, and the terms of any such
- 4 implied contract; and,
- 5 p. Whether Defendants breached the implied contract.

6 **CLAIMS ALLEGED ON BEHALF OF THE CLASS**

7 **First Claim for Relief**

8 **Violation of California’s Unfair Competition Law (“UCL”)**

9 **Unlawful Business Practice**

10 **(Cal. Bus. & Prof. Code § 17200, *et seq.*)**

11 **(On Behalf of Plaintiffs, the Nationwide Class,**

12 **the Best Buy Subclass, and the Delta Subclass)**

13 103. Plaintiffs repeat, reallege, and incorporate by reference the allegations

14 contained in paragraphs 1 through 102 as though fully stated herein.

15 104. By reason of the conduct alleged herein, Defendants engaged in unlawful

16 “business practices” within the meaning of the UCL.

17 105. Since at least September 2017, 24/7 has been the customer support provider

18 and agent of Best Buy and Delta to provide customer service support to their respective

19 customers. 24/7 is the agent of both Best Buy and Delta.

20 106. 24/7 stored the Customer Data of Plaintiffs and the Class and Subclass

21 members on behalf of Best Buy and Delta in its computer systems. Defendants falsely

22 represented to Plaintiffs and the Class and Subclass members that their Customer Data was

23 secure and would remain private.

24 107. Defendants knew or should have known they did not employ reasonable,

25 industry standard, and appropriate security measures that complied “with federal

26 regulations” and that would have kept Plaintiffs’ and the Class and Subclass members’

27 Customer Data secure and prevented the loss or misuse of that Customer Data.

28

1           108. Even without these misrepresentations, Plaintiffs and the Class and Subclass  
2 members were entitled to assume, and did assume Defendants would take appropriate  
3 measures to keep their Customer Data safe. Defendants did not disclose at any time that  
4 Plaintiffs' Customer Data was vulnerable to hackers because Defendants' data security  
5 measures were inadequate and outdated, and Defendants were the only ones in possession  
6 of that material information, which they had a duty to disclose. Defendants violated the  
7 UCL by misrepresenting, both by affirmative conduct and by omission, the safety of their  
8 computer systems, specifically the security thereof, and their ability to safely store  
9 Plaintiffs' and the Class and Subclass members' Customer Data. Defendants also violated  
10 the UCL by failing to implement reasonable and appropriate security measures or follow  
11 industry standards for data security, failing to comply with their own posted privacy  
12 policies, and by failing to immediately notify Plaintiffs and the Class and Subclass  
13 members of the Data Breach. If Defendants had complied with these legal requirements,  
14 Plaintiffs and the Class and Subclass members would not have suffered the damages related  
15 to the Data Breach, and consequently from, Defendants' failure to timely notify Plaintiffs  
16 and the Class and Subclass members of the Data Breach.  
17  
18

19           109. Defendants' acts, omissions, and misrepresentations as alleged herein were  
20 unlawful and in violation of, *inter alia*, Section 5(a) of the Federal Trade Commission Act.

21           110. Plaintiffs and the Class and Subclass members suffered injury in fact and  
22 lost money or property as the result of Defendants' unlawful business practices. In  
23 particular, Plaintiffs and the Class and Subclass members have suffered from improper or  
24 fraudulent charges to their credit/debit card accounts; and other similar harm, all as a result  
25 of the Data Breach. In addition, their Customer Data was taken and is in the hands of those  
26 who will use it for their own advantage, or is being sold for value, making it clear that the  
27  
28

1 hacked information is of tangible value. Plaintiffs and the Class and Subclass members  
2 have also suffered consequential out of pocket losses for procuring credit freeze or  
3 protection services, identity theft monitoring, and other expenses relating to identity theft  
4 losses or protective measures.

5 111. As a result of Defendants' unlawful business practices, violations of the  
6 UCL, Plaintiffs and the Class and Subclass members are entitled to injunctive relief.

7  
8 **Second Claim for Relief**  
9 **Violation of California's Unfair Competition Law ("UCL")**  
10 **Unfair Business Practice**  
11 **(Cal. Bus. & Prof. Code § 17200, *et seq.*)**  
12 **(On Behalf of Plaintiffs, the Nationwide Class,**  
13 **the Best Buy Subclass, and the Delta Subclass)**

14 112. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
15 contained in paragraphs 1 through 102 as though fully stated herein.

16 113. By reason of the conduct alleged herein, Defendants engaged in unfair  
17 "business practices" within the meaning of the UCL.

18 114. Defendants stored Plaintiffs' and the Class and Subclass members'  
19 Customer Data in their electronic and consumer information databases. Defendants  
20 represented to Plaintiffs and the Class and Subclass members that their Customer Data  
21 databases were secure and that Plaintiffs' and the Class and Subclass members' Customer  
22 Data would remain private. Best Buy and Delta, themselves and through their agent 24/7,  
23 engaged in unfair acts and business practices by representing that they had secure computer  
24 systems when they did not.

25 115. Even without these misrepresentations, Plaintiffs and the Class and Subclass  
26 members were entitled to, and did, assume Defendants would take appropriate measures to  
27 keep their Customer Data safe. Defendants did not disclose at any time that Plaintiffs'  
28 Customer Data was vulnerable to hackers because Defendants' data security measures were

1 inadequate and outdated, and Defendants were the only ones in possession of that material  
2 information, which they had a duty to disclose.

3 116. Defendants knew or should have known they did not employ reasonable  
4 measures that would have kept Plaintiffs' and the Class and Subclass members' Customer  
5 Data secure and prevented the loss or misuse of Plaintiffs' and the Class and Subclass  
6 members' Customer Data.

7 117. Defendants violated the UCL by misrepresenting, both by affirmative  
8 conduct and by omission, the security of their systems and services, and their ability to  
9 safely store Plaintiffs' and the Class and Subclass members' Customer Data. Defendants  
10 also violated the UCL by failing to implement and maintain reasonable security procedures  
11 and practices appropriate to protect Customer Data, and by failing to immediately notify  
12 Plaintiffs and the Class and Subclass members of the Data Breach.

13 118. Defendants also violated their commitment to maintain the confidentiality  
14 and security of Plaintiffs' and the Class and Subclass members' Customer Data, and failed  
15 to comply with their own policies and applicable laws, regulations, and industry standards  
16 relating to data security.

17 119. **Defendants engaged in unfair business practices under the “balancing**  
18 **test.”** The harm caused by Defendants' actions and omissions, as described in detail above,  
19 greatly outweigh any perceived utility. Indeed, Defendants' failure to follow basic data  
20 security protocols and misrepresentations to consumers about Defendants' data security  
21 cannot be said to have had any utility at all. All of these actions and omissions were clearly  
22 injurious to Plaintiffs and the Class and Subclass members, directly causing the harms  
23 alleged below.  
24  
25  
26  
27  
28

1           **120. Defendants engaged in unfair business practices under the “tethering**  
2 **test.”** Defendants’ actions and omissions, as described in detail above, violated  
3 fundamental public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ.  
4 Code § 1798.1 (“The Legislature declares that ... all individuals have a right of privacy in  
5 information pertaining to them.... The increasing use of computers ... has greatly magnified  
6 the potential risk to individual privacy that can occur from the maintenance of personal  
7 information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the Legislature to ensure  
8 that personal information about California residents is protected.”); Cal. Bus. & Prof. Code  
9 § 22578 (“It is the intent of the Legislature that this chapter [including the Online Privacy  
10 Protection Act] is a matter of statewide concern.”) Defendants’ acts and omissions, and the  
11 injuries caused by them, are thus “comparable to or the same as a violation of the law ...”  
12 *Cel-Tech Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th  
13 163, 187.  
14

15           **121. Defendants engaged in unfair business practices under the “FTC test.”**  
16 The harm caused by Defendants’ actions and omissions, as described in detail above, is  
17 substantial in that it affects hundreds of thousands of Class and Subclass members and has  
18 caused those persons to suffer actual harms. Such harms include a substantial risk of  
19 identity theft, disclosure of Plaintiffs’ and the Class and Subclass members’ Customer Data  
20 to third parties without their consent, diminution in value of their Customer Data,  
21 consequential out of pocket losses for procuring credit freeze or protection services,  
22 identity theft monitoring, and other expenses relating to identity theft losses or protective  
23 measures. This harm continues given the fact that Plaintiffs’ and the Class and Subclass  
24 members’ Customer Data remains in Defendants’ possession, without adequate protection,  
25 and is also in the hands of those who obtained it without their consent. Defendants’ actions  
26  
27  
28

1 and omissions violated, *inter alia*, Section 5(a) of the Federal Trade Commission Act, 15  
2 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613  
3 (D.N.J. 2014), *aff'd*, 799 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No.  
4 9357, FTC File No. 102-3099 (July 28, 2016) (failure to employ reasonable and  
5 appropriate measures to secure personal information collected violated § 5(a) of FTC Act);  
6 *In re BJ's Wholesale Club, Inc.*, FTC Docket No. C-4148, FTC File No. 042-3160 (Sept.  
7 20, 2005) (same); *In re CardSystems Solutions, Inc.*, FTC Docket No. C-4168, FTC File  
8 No. 052-3148 (Sept. 5, 2006) (same); *see also United States v. ChoicePoint, Inc.*, Civil  
9 Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct. 14, 2009) (“failure to establish and  
10 implement, and thereafter maintain, a comprehensive information security program that is  
11 reasonably designed to protect the security, confidentiality, and integrity of personal  
12 information collected from or about consumers” violates § 5(a) of FTC Act); 15 U.S.C. §  
13 45(n) (defining “unfair acts or practices” as those that “cause[ ] or [are] likely to cause  
14 substantial injury to consumers which [are] not reasonably avoidable by consumers  
15 themselves and not outweighed by countervailing benefits to consumers or to  
16 competition.”).

19 122. Plaintiffs and the Class and Subclass members suffered injury in fact and  
20 lost money or property as the result of Defendants’ unfair business practices. In particular,  
21 Plaintiffs and the Class and Subclass members have suffered from improper or fraudulent  
22 charges to their credit/debit card accounts; and other similar harm, all as a result of the Data  
23 Breach. In addition, their Customer Data was taken and is in the hands of those who will  
24 use it for their own advantage, or is being sold for value, making it clear that the hacked  
25 information is of tangible value. Plaintiffs and the Class and Subclass members have also  
26 suffered consequential out of pocket losses for procuring credit freeze or protection  
27  
28

1 services, identity theft monitoring, and other expenses relating to identity theft losses or  
2 protective measures.

3 123. As a result of Defendants' unfair business practices, violations of the UCL,  
4 Plaintiffs and the Class and Subclass members are entitled to injunctive relief.

5 **Third Claim for Relief**  
6 **Negligence**  
7 **(On Behalf of Plaintiffs, the Nationwide Class,**  
8 **the Best Buy Subclass, and the Delta Subclass)**

9 124. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
10 contained in paragraphs 1 through 102 as though fully stated herein.

11 125. Upon accepting and storing Plaintiffs' and the Class and Subclass members'  
12 Customer Data in their computer systems and on their networks, Defendants undertook and  
13 owed a duty to Plaintiffs and the Class and Subclass members to exercise reasonable care  
14 to secure and safeguard that information and to use commercially reasonable methods to do  
15 so. Defendants knew that the Customer Data was private and confidential, and should be  
16 protected as private and confidential. 24/7 owed this duty to the Nationwide Class, as well  
17 as the Best Buy and Delta Subclasses; Best Buy owed this duty to the Best Buy Subclass;  
18 and Delta owed this duty to the Delta Subclass.

19 126. Defendants owed these respective duties of care not to subject Plaintiffs and  
20 the Class and Subclass members, along with their Customer Data, to an unreasonable risk  
21 of harm because they were foreseeable and probable victims of any inadequate security  
22 practices.

23 127. Defendants owed a duty to Plaintiffs and the Class and Subclass members to  
24 exercise reasonable care in safeguarding and protecting their Customer Data and keeping it  
25 from being compromised, lost, stolen, misused, and or/disclosed to unauthorized parties.  
26 This duty included, among other things, designing, maintaining, and testing Defendants'  
27 security systems to ensure Plaintiffs' and the Class and Subclass members' Customer Data  
28 was adequately secured and protected. Defendants further had a duty to implement  
processes that would detect a breach of their data system in a timely manner. 24/7 owed

1 these duties to the Nationwide Class, as well as the Best Buy and Delta Subclasses; Best  
2 Buy owed these duties to the Best Buy Subclass; and Delta owed these duties to the Delta  
3 Subclass.

4 128. Defendants knew that Plaintiffs' and the Class and Subclass members'  
5 Customer Data was personal and sensitive information that is valuable to identity thieves  
6 and other criminals. Defendants also knew of the serious harms that could happen if  
7 Plaintiffs' and the Class and Subclass members' Customer Data was wrongfully disclosed,  
8 that disclosure was not fixed, or Plaintiffs and the Class and Subclass members were not  
9 told about the disclosure in a timely manner.

10 129. By being entrusted by Plaintiffs and the Class and Subclass members to  
11 safeguard their respective Customer Data, Defendants had special relationships with  
12 Plaintiffs and the Class and Subclass members; Plaintiffs and the Class and Subclass  
13 members utilized 24/7 product, and patronized Best Buy and Delta, and accepted Best  
14 Buy's and Delta's respective offers to use payment cards as an approved form of payment  
15 through 24/7's customer support platform. Plaintiffs and the Class and Subclass members  
16 did so with the understanding that Defendants would take appropriate measures to protect  
17 their respective Customer Data and would inform Plaintiffs and the Class and Subclass  
18 members of any breaches or other security concerns that might call for action. But,  
19 Defendants did not. Defendants not only knew their data security was inadequate, they also  
20 knew they didn't have the tools to detect and document intrusions or exfiltration of  
21 Customer Data. Defendants are morally culpable, given their wholly inadequate safeguards,  
22 as well as their refusal to notify Plaintiffs and the Class and Subclass members of breaches  
23 or security vulnerabilities.

24 130. Defendants breached their respective duties to exercise reasonable care in  
25 safeguarding and protecting Plaintiffs' and the Class and Subclass members' Customer  
26 Data by failing to adopt, implement, and maintain adequate security measures to safeguard  
27 that information, and allowing unauthorized access to Plaintiffs' and the Class and Subclass  
28 members' Customer Data.

1           131. Defendants also breached their respective duties to timely disclose that  
2 Plaintiffs' and the Class and Subclass members' Customer Data had been, or was  
3 reasonably believed to have been, stolen, exposed, or compromised.

4           132. Defendants' failure to comply with industry further evidences Defendants'  
5 negligence in failing to exercise reasonable care in safeguarding and protecting Plaintiffs'  
6 and the Class and Subclass members' Customer Data.

7           133. But for Defendants' respective wrongful and negligent breach of their  
8 respective duties owed to Plaintiffs and the Class and Subclass members, their Customer  
9 Data would not have been compromised, stolen, and viewed by unauthorized persons.  
10 Defendants' respective negligence was a direct and legal cause of the theft of Plaintiffs'  
11 and the Class and Subclass members' Customer Data, as well as the resulting damages.

12           134. The injury and harm Plaintiffs and the Class and Subclass members suffered  
13 was the reasonably foreseeable result of Defendants' respective failure to exercise  
14 reasonable care in safeguarding and protecting Plaintiffs' and the Class and Subclass  
15 members' Customer Data. Defendants knew their computer systems and technologies for  
16 accepting and securing Plaintiffs' and the Class and Subclass members' Customer Data had  
17 numerous security vulnerabilities.

18           135. Defendants' respective misconduct as alleged herein was willful and with  
19 conscious disregard of Plaintiffs' and the Class and Subclass members' rights or safety, and  
20 despicable conduct that has subjected Plaintiffs and the Class and Subclass members to  
21 cruel and unjust hardship in conscious disregard of their rights.

22           136. As a result of Defendants' respective misconduct, Plaintiffs' and the Class  
23 and Subclass members' Customer Data was compromised, placing them at a greater risk of  
24 identity theft and subjecting them to identity theft, and their Customer Data was disclosed  
25 to third parties without their consent. Plaintiff and the Class and Subclass members also  
26 suffered diminution in value of their Customer Data in that it is now easily available to  
27 hackers on the dark web. Plaintiffs and the Class and Subclass members have also suffered  
28 consequential out of pocket losses for procuring credit freeze or protection services,

1 identity theft monitoring, and other expenses relating to identity theft losses or protective  
2 measures.

3 **Fourth Claim for Relief**  
4 **Breach of Implied Contract**  
5 **(On Behalf of Plaintiffs, the Best Buy Subclass, and the Delta Subclass)**

6 137. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
7 contained in paragraphs 1 through 102 as though fully stated herein.

8 138. Best Buy solicited and invited the Best Buy Plaintiff and the Best Buy  
9 Subclass members to use the electronic customer support platform to make purchases using  
10 their credit or debit cards. The Best Buy Plaintiff and the Best Buy Subclass members  
11 accepted Best Buy's offer and used their credit or debit cards to patronize Best Buy during  
12 the period of the Data Breach.

13 139. Delta solicited and invited the Delta Plaintiff and the Delta Subclass  
14 members to use the electronic customer support platform to make purchases using their  
15 credit or debit cards. The Delta Plaintiff and the Delta Subclass members accepted Delta's  
16 offer and used their credit or debit cards to patronize Delta during the period of the Data  
17 Breach.

18 140. When Plaintiffs and the Subclass members respectively patronized Best Buy  
19 and Delta using payment cards, they provided their Customer Data, including but not  
20 limited to the PII of their debit and credit cards. In so doing, Plaintiffs and the Subclass  
21 members entered into implied contracts with Best Buy and Delta, respectively, pursuant to  
22 which Best Buy and Delta, respectively, agreed to safeguard and protect such information  
23 and to timely and accurately notify Plaintiffs and the Subclass members if their data had  
24 been breached and compromised.

25 141. Each purchase Plaintiffs and the Subclass members made at Best Buy or  
26 Delta, respectively, using their credit or debit card was made pursuant to the mutually  
27 agreed-upon implied contract with that Defendant, under which that Defendant agreed to  
28 safeguard and protect the Customer Data of Plaintiffs and the Subclass members, including

1 Plaintiffs' and the Subclass members' PII and credit or debit cards, and to timely and  
2 accurately notify them if such information was compromised or stolen.

3 142. Plaintiffs and the Subclass members would not have provided and entrusted  
4 their Customer Data, including PII and credit and debit card information, to the respective  
5 Defendant to make purchases in the absence of the implied contract between them and the  
6 respective Defendant.

7 143. Plaintiffs and the Subclass members fully performed their obligations under  
8 the respective implied contracts with Defendants.

9 144. Defendants breached the respective implied contracts made with Plaintiffs  
10 and the Subclass members by failing to safeguard and protect Plaintiffs' and the Subclass  
11 members' Customer Data by failing to provide timely and accurate notice to them that their  
12 Customer Data was compromised as a result of the Data Breach.

13 145. As a direct and proximate result of Defendants' breaches of the implied  
14 contracts, Plaintiffs and the Subclass members sustained actual losses and damages,  
15 including nominal damages, as described in detail above. These breaches of implied  
16 contracts were a direct and legal cause of the injuries and damages to Plaintiffs and the  
17 Subclass members, as described above.

18 **Fifth Claim for Relief**  
19 **Negligence Per Se**  
20 **(On Behalf of Plaintiffs, the Nationwide Class,**  
21 **the Best Buy Subclass, and the Delta Subclass)**

22 146. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
23 contained in paragraphs 1 through 102 as though fully stated herein.

24 147. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting  
25 commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by  
26 businesses, such as Defendants, of failing to use reasonable measures to protect Customer  
27 Data.

28 148. Defendants violated Section 5 of the FTC Act by failing to use reasonable  
measures to protect Customer Data and not complying with applicable industry standards.

1 Defendants' conduct was particularly unreasonable given the nature and amount of  
2 Customer Data they obtained and stored, and the foreseeable consequences of a data breach  
3 at Best Buy and Delta, including, specifically, the immense damages that would result to  
4 Plaintiffs and the Class and Subclass members.

5 149. Defendants' violation of Section 5 of the FTC Act constitutes negligence  
6 *per se*.

7 150. Plaintiffs and the Class and Subclass members are within the class of  
8 persons the FTC Act was intended to protect.

9 151. The harm that occurred as a result of the Data Breach is the type of harm the  
10 FTC Act was intended to guard against. The FTC has pursued enforcement actions against  
11 businesses, which, as a result of their failure to employ reasonable data security measures  
12 and avoid unfair and deceptive practices, caused the same harm as that Plaintiffs and the  
13 Class and Subclass members suffered.

14 152. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs  
15 and the Class and Subclass members have suffered, and continue to suffer, injuries and  
16 damages arising from Plaintiffs' and the Class and Subclass members' inability to use their  
17 debit or credit cards because those cards were cancelled, suspended, or otherwise rendered  
18 unusable as a result of the Data Breach and/or false or fraudulent charges stemming from  
19 the Data Breach, including but not limited to late fees charged and foregone cash back  
20 rewards; damages from lost time and effort to mitigate the actual and potential impact of  
21 the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with  
22 credit reporting agencies, contacting their financial institutions, closing or modifying  
23 financial accounts, closely reviewing and monitoring their credit reports and accounts for  
24 unauthorized activity, and filing police reports and damages from identity theft, which may  
25 take months if not years to discover and detect, given the far-reaching, adverse and  
26 detrimental consequences of identity theft and loss of privacy.

**Sixth Claim for Relief**  
**Unjust Enrichment**  
**(On Behalf of Plaintiffs, the Nationwide Class,**  
**the Best Buy Subclass, and the Delta Subclass)**

1  
2  
3       153. Plaintiffs repeat, reallege, and incorporate by reference the allegations  
4 contained in paragraphs 1 through 102 as though fully stated herein.

5       154. Plaintiffs and the Class and Subclass members conferred a monetary benefit  
6 on Defendants. Specifically, the Best Buy Plaintiff and the Best Buy Subclass patronized  
7 and provided Best Buy with their payment information through Best Buy's agent 24/7. In  
8 exchange, the Best Buy Plaintiff and the Best Buy Subclass members should have received  
9 from Best Buy the goods and services that were the subject of the transaction and should  
10 have been entitled to have Best Buy and its agent 24/7 protect their Customer Data with  
11 adequate data security.

12       155. Also, the Delta Plaintiff and the Delta Subclass members patronized and  
13 provided Delta with their payment information through Delta's agent 24/7. In exchange,  
14 the Delta Plaintiff and the Delta Subclass members should have received from Delta the  
15 goods and services that were the subject of the transaction and should have been entitled to  
16 have Delta and its agent 24/7 protect their Customer Data with adequate data security.

17       156. Further, the Plaintiffs and the Class members provided 24/7 with their  
18 payment information and Customer Data, to be provided to 24/7's principals. In exchange,  
19 the Plaintiffs and the Class members should have received from 24/7's principals the goods  
20 and services that were the subject of the transaction and should have been entitled to have  
21 those principals and their agent 24/7 protect their Customer Data with adequate data  
22 security.

23       157. Defendants knew that the respective Plaintiffs and the Class and Subclass  
24 members conferred those benefits on the respective Defendant, and the respective  
25 Defendant accepted or retained that benefit. Defendants profited from the purchases and  
26 used Plaintiffs' and the Class and Subclass members' Customer Data for business purposes.  
27  
28



- 1 b. Finding that Defendants' conduct was negligent, deceptive, unfair, and  
2 unlawful as alleged herein;
- 3 c. Enjoining Defendants from engaging in further negligent, deceptive, unfair,  
4 and unlawful business practices alleged herein;
- 5 d. Awarding Plaintiffs and the Class and Subclass members actual,  
6 compensatory, consequential, and/or nominal damages;
- 7 e. Awarding Plaintiffs and the Class and Subclass members statutory damages  
8 and penalties, as allowed by law;
- 9 f. Requiring Defendants to provide appropriate credit monitoring services to  
10 Plaintiffs and the Class and Subclass members;
- 11 g. Compelling Defendants to use appropriate cyber security methods and  
12 policies with respect to data collection, storage, and protection, and to  
13 disclose with specificity to the Class and Subclass members the type of  
14 Customer Data compromised;
- 15 h. Awarding Plaintiffs and the Class and Subclass members pre-judgment and  
16 post-judgment interest;
- 17 i. Awarding Plaintiffs and the Class and Subclass members reasonable  
18 attorneys' fees, costs and expenses, and;
- 19 j. Granting such other relief as the Court deems just and proper.

20  
21 Dated: May 10th, 2018

/s/ Joshua H. Watson

CLAYEO C. ARNOLD  
California SBN 65070  
carnold@justice4you.com  
JOSHUA H. WATSON  
California SBN 238058  
Email: jwatson@justice4you.com  
CLAYEO C. ARNOLD, A PROFESSIONAL  
LAW CORPORATION  
865 Howe Avenue  
Sacramento, California 95825  
Telephone: (916) 777-7777  
Facsimile: (916) 924-1829

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

JOHN A. YANCHUNIS\*  
jyanchunis@ForThePeople.com  
RYAN J. MCGEE\*  
rmcgee@ForThePeople.com  
MORGAN & MORGAN  
COMPLEX LITIGATION GROUP  
201 N. Franklin Street, 7th Floor  
Tampa, Florida 33602  
Telephone: (813) 223-5505  
Facsimile: (813) 223-5402

*Attorneys for Plaintiff and the Proposed Class*

\* *pro hac vice* application to be submitted

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
MICHAEL FORD and RUDOLPH DUBROVSZKY
(b) County of Residence of First Listed Plaintiff Kendall County, TX
(c) Attorneys (Firm Name, Address, and Telephone Number)
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION
865 Howe Avenue, Sacramento, California 95825, Telephone: (916) 777-7777

DEFENDANTS
24/7, INC., BEST BUY CO., INC., and DELTA AIRLINES, INC.
County of Residence of First Listed Defendant
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
4 Diversity

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)
Citizen of This State
Citizen of Another State
Citizen or Subject of a Foreign Country
PTF DEF
1 1
2 2
3 3
4 4
5 5
6 6

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

Table with 5 columns: CONTRACT, REAL PROPERTY, TORTS, CIVIL RIGHTS, PRISONER PETITIONS, FORFEITURE/PENALTY, LABOR, IMMIGRATION, BANKRUPTCY, SOCIAL SECURITY, FEDERAL TAX SUITS, OTHER STATUTES. Includes categories like Insurance, Marine, Negotiable Instrument, etc.

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
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):
Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)
Brief description of cause:
Violation of California's Unfair Competition Law

VII. REQUESTED IN COMPLAINT:
CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, Fed. R. Civ. P. DEMAND \$ 5,000,000.00
CHECK YES only if demanded in complaint: JURY DEMAND: Yes No

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

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)
SAN FRANCISCO/OAKLAND SAN JOSE EUREKA-MCKINLEYVILLE

DATE 05/10/2018 SIGNATURE OF ATTORNEY OF RECORD /s/ Joshua H. Watson

## 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.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

MICHAEL FORD and RUDOLPH DUBROVSZKY,
individually and on behalf of all others similarly
situated,

Plaintiff(s)

v.

24/7, INC., a California Corporation, BEST BUY CO.,
INC., a Minnesota corporation, and DELTA
AIRLINES, INC., a Delaware corporation,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address) 24/7, INC.
Registered Agent JAY NASH
248 SILVER OAK DR
PASO ROBLES CA 93446

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you
are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ.
P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of
the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney,
whose name and address are:

Clayeo C. Arnold, California SBN 65070
Joshua H. Watson, California SBN 238058
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint.
You also must file your answer or motion with the court.

CLERK OF COURT

Date: \_\_\_\_\_

Signature of Clerk or Deputy Clerk

Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_ .

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* \_\_\_\_\_  
\_\_\_\_\_, a person of suitable age and discretion who resides there,  
on *(date)* \_\_\_\_\_ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* \_\_\_\_\_ , who is  
designated by law to accept service of process on behalf of *(name of organization)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I returned the summons unexecuted because \_\_\_\_\_ ; or

Other *(specify)*: \_\_\_\_\_

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ \_\_\_\_\_ 0.00 \_\_\_\_\_ .

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

**Print**

**Save As...**

**Reset**

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

MICHAEL FORD and RUDOLPH DUBROVSZKY,
individually and on behalf of all others similarly
situated,

Plaintiff(s)

v.

24/7, INC., a California Corporation, BEST BUY CO.,
INC., a Minnesota corporation, and DELTA
AIRLINES, INC., a Delaware corporation,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address) BEST BUY CO., INC.
Registered Agent CT Corporation System, Inc.
1010 Dale St N
St Paul, MN 55117-5603

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you
are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ.
P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of
the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney,
whose name and address are:

Clayeo C. Arnold, California SBN 65070
Joshua H. Watson, California SBN 238058
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint.
You also must file your answer or motion with the court.

CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk

Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_ .

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* \_\_\_\_\_  
\_\_\_\_\_, a person of suitable age and discretion who resides there,  
on *(date)* \_\_\_\_\_ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* \_\_\_\_\_ , who is  
designated by law to accept service of process on behalf of *(name of organization)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I returned the summons unexecuted because \_\_\_\_\_ ; or

Other *(specify)*: \_\_\_\_\_

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ \_\_\_\_\_ 0.00 \_\_\_\_\_ .

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

**Print**

**Save As...**

**Reset**

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Northern District of California

MICHAEL FORD and RUDOLPH DUBROVSZKY,
individually and on behalf of all others similarly
situated,

Plaintiff(s)

v.

24/7, INC., a California Corporation, BEST BUY CO.,
INC., a Minnesota corporation, and DELTA
AIRLINES, INC., a Delaware corporation,

Defendant(s)

Civil Action No.

SUMMONS IN A CIVIL ACTION

To: (Defendant's name and address) DELTA AIRLINES, INC.
Registered Agent Corporation Service Company
251 Little Falls Drive
Wilmington, DE 19808

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you
are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ.
P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of
the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney,
whose name and address are:

Clayeo C. Arnold, California SBN 65070
Joshua H. Watson, California SBN 238058
CLAYEO C. ARNOLD, A PROFESSIONAL LAW CORPORATION
865 Howe Avenue
Sacramento, California 95825
Telephone: (916) 777-7777
Facsimile: (916) 924-1829

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint.
You also must file your answer or motion with the court.

CLERK OF COURT

Date:

Signature of Clerk or Deputy Clerk

Civil Action No. \_\_\_\_\_

**PROOF OF SERVICE**

*(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))*

This summons for *(name of individual and title, if any)* \_\_\_\_\_  
was received by me on *(date)* \_\_\_\_\_ .

I personally served the summons on the individual at *(place)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I left the summons at the individual's residence or usual place of abode with *(name)* \_\_\_\_\_  
\_\_\_\_\_, a person of suitable age and discretion who resides there,  
on *(date)* \_\_\_\_\_ , and mailed a copy to the individual's last known address; or

I served the summons on *(name of individual)* \_\_\_\_\_ , who is  
designated by law to accept service of process on behalf of *(name of organization)* \_\_\_\_\_  
\_\_\_\_\_ on *(date)* \_\_\_\_\_ ; or

I returned the summons unexecuted because \_\_\_\_\_ ; or

Other *(specify)*:

My fees are \$ \_\_\_\_\_ for travel and \$ \_\_\_\_\_ for services, for a total of \$ \_\_\_\_\_ 0.00 \_\_\_\_\_ .

I declare under penalty of perjury that this information is true.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Server's signature*

\_\_\_\_\_  
*Printed name and title*

\_\_\_\_\_  
*Server's address*

Additional information regarding attempted service, etc:

**Print**

**Save As...**

**Reset**

# ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Customer Service Chat Co. 24/7 Named Alongside Best Buy, Delta Airlines in Data Breach Class Action](#)

---