

1 Michael F. Ram, SBN #104805  
mram@rocklawcal.com  
2 Matt Malone, SBN #221545  
mjm@rocklawcal.com  
3 RAM, OLSON, CEREGHINO  
4 & KOPCZYNSKI LLP  
101 Montgomery Street, Suite 1800  
5 San Francisco, California 94104  
Telephone: (415) 433-4949  
6 Facsimile: (415) 433-7311

7 [Additional Counsel Listed On Signature Page]

8 *Attorneys for Plaintiff and Proposed Class*

9  
10 **UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF CALIFORNIA**

11 LEE WALTERS, individually and on behalf of  
12 all others similarly situated,

13 Plaintiff,

14 v.

15 KIMPTON HOTEL & RESTAURANT  
16 GROUP, LLC

17 Defendant.

Case No. 3:16-cv-05387-VC

**AMENDED CLASS ACTION  
COMPLAINT FOR:**

- 1) Breach of Implied Contract
- 2) Violation of the California Unfair Competition Law, Business & Professions Code § 17200, *et seq.*
- 3) Negligence

**JURY TRIAL DEMAND**

21  
22 Plaintiff Lee Walters brings this Amended Class Action Complaint against Kimpton  
23 Hotel & Restaurant Group, LLC, on behalf of himself and all others similarly situated, and  
24 alleges, upon personal knowledge as to his own actions and his counsel’s investigations, and  
25 upon information and belief as to all other matters, as follows:  
26  
27

1 **NATURE OF THE ACTION**

2 1. Plaintiff brings this class action against Kimpton Hotel & Restaurant Group,  
3 LLC (referred to herein as “Kimpton” or “Defendant”) for its failure to secure and safeguard its  
4 customers’ credit and debit card numbers and other payment card data (“PCD”), personally  
5 identifiable information (“PII”) such as the cardholders’ names, mailing addresses, and other  
6 personal information, which Kimpton collected at the time of check-in to one of its hotels, or  
7 use at one its retail operations within its hotels (collectively, “Private Information”), and for  
8 failing to provide timely, accurate, and adequate notice to Plaintiff and other Class members  
9 that their Private Information had been stolen, as well as precisely what types of information  
10 were stolen. When consumers use their payment cards at Kimpton, Kimpton electronically  
11 collects and stores this information, making it a treasure trove of useful information attractive  
12 to hackers who can use the information to profit and cause damage, as was done here, to  
13 consumers.

14 2. Beginning in or around February 16, 2016 and perhaps ever earlier and  
15 continuing through July 7, 2016, hackers utilizing malware accessed the computer systems at  
16 Kimpton hotels in numerous locations throughout the United States, including California, and  
17 stole copies of Kimpton customers’ Private Information (the “Data Breach”). While copied,  
18 Plaintiff’s and consumers’ information remains in the possession of Kimpton. On July 26,  
19 2016, Kimpton announced it may have sustained a data breach.

20 3. On August 31, 2016, Kimpton acknowledged that it discovered malicious  
21 software designed to steal credit card data on computers that operate the payment processing  
22 systems for Kimpton hotels and restaurants. [https://www.kimptonhotels.com/promos/payment-](https://www.kimptonhotels.com/promos/payment-card-notification)  
23 [card-notification](https://www.kimptonhotels.com/promos/payment-card-notification). Kimpton released additional information stating that the at-risk window  
24 began on February 16, 2016 through July 7, 2016, and that the malware was designed to collect  
25 payment card data—cardholder name, card number, expiration date and internal verification  
26  
27

1 code—from cards used in connection with activities at the hotels. The information collected  
2 included PCD (payment card data). In this same press release, Kimpton acknowledged its  
3 obligation to safeguard its customers’ information: “Kimpton Hotels & Restaurants values the  
4 relationship we have with our guests and understands the importance of protecting personal  
5 information. We are notifying you of an incident that may involve your payment card  
6 information.” Kimpton released very few details, and it did not explain why it had delayed  
7 notification of the public regarding the Data Breach.

8 4. On September 9, 2016, Kimpton sent letters to customers who had visited its  
9 properties during the affected period and who had used their payment cards to make purchases  
10 for goods and services. Plaintiff received such a letter. A true and correct copy is attached.

11 5. Kimpton could have prevented this Data Breach. The malicious software used in  
12 the Data Breach was more than likely a variant of “BlackPOS,” the identical malware strain  
13 that hackers used in data breaches at many other hotel chains, including Hilton, Starwood,  
14 Mandarin Oriental, White Lodging (on two occasions), and the Trump Collection. While many  
15 retailers, banks, and card companies responded to recent breaches by adopting technology that  
16 helps makes transactions more secure, Kimpton acknowledged twice in its press releases  
17 discussing the Data Breach that Kimpton did not do so until it was too late. Although Kimpton  
18 claims it has now strengthen its existing security measures,  
19 <https://www.kimptonhotels.com/promos/payment-card-notification>, the quality of the measures  
20 taken remains suspect and the need for judicial intervention and consumer and independent  
21 oversight is mandated by the circumstances described herein.

22 6. Kimpton disregarded Plaintiff’s and Class members’ rights by intentionally,  
23 willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure  
24 its data systems were protected, failing to take available steps to prevent and stop the breach  
25 from ever happening, and failing to disclose to its customers the material facts that it did not  
26  
27

1 have adequate computer systems and security practices to safeguard customers' Private  
2 Information. On information and belief, Plaintiff's and Class members' Private Information  
3 was improperly handled and stored, was unencrypted, and was not kept in accordance with  
4 applicable, required, and appropriate cyber-security protocols, policies, and procedures. As a  
5 result, Plaintiff's and Class members' Private Information was compromised and stolen.  
6 However, as this same information remains stored in Kimpton's computer systems, Plaintiff  
7 and class members have an interest in ensuring that their information is safe, and they should  
8 be entitled to seek injunctive and other equitable relief, including independent oversight of  
9 Kimpton's security systems.

#### 10 **PARTIES**

11 7. Plaintiff Lee Walters is an individual and resident of California.

12 8. Kimpton Hotels & Restaurants, LLC is a California corporation with its  
13 principle place of business in San Francisco. Kimpton primarily derives its revenues from  
14 hotel and restaurant operations.

#### 15 **JURISDICTION AND VENUE**

16 9. This Court has jurisdiction over this action under the Class Action Fairness Act,  
17 28 U.S.C. § 1332(d). The aggregated claims of the individual class members exceed  
18 \$5,000,000.00, exclusive of interest and costs, and this is a class action in which more than  
19 two-thirds of the proposed plaintiff class, on the one hand, and Kimpton, on the other, are  
20 citizens of different states.

21 10. This Court has jurisdiction over Kimpton as it maintains its corporate  
22 headquarters in this District and for the following reasons: Kimpton makes decisions regarding  
23 overall corporate governance and management with regards to the hotels that it owns or  
24 manages, including the security measures to protect its customers' Private Information, in this  
25 District; it is authorized to conduct business throughout the United States, including California;  
26  
27

1 it owns and operates many hotels throughout California and the United States; and it advertises  
2 in a variety of media throughout the United States, including California. Via its business  
3 operations throughout the United States, Kimpton intentionally avails itself of the markets  
4 within this state to render the exercise of jurisdiction by this Court just and proper.

5 11. Venue is proper in this District pursuant to 28 U.S.C. § 1391(a)(1) because a  
6 substantial part of the events and omissions giving rise to this action occurred in this District  
7 and because Kimpton is headquartered in this District.

### 8 **FACTUAL BACKGROUND**

#### 9 **A. Plaintiff's Individual Facts**

10 12. On December 28, 2015, and on May 29, 2016, Plaintiff used his payment card  
11 when checking into two different Kimpton Hotels located in California. In April, 2016, he  
12 sustained a breach of the payment card used to book his stay on December 28, 2015 when he  
13 discovered that card had been used to purchase tickets on line to Disneyland. At the time of this  
14 purchase, which he neither authorized nor made, the credit card used was in his possession and  
15 control. As a result of this fraudulent charge, Plaintiff replaced his payment card at his bank.

16 13. When Plaintiff booked and paid for his stay on May 29, 2016, at another  
17 Kimpton he used a second payment card. While he has not noticed any fraudulent activity on  
18 this card, he takes time out of his life monitors his credit through an identity theft protection  
19 service to ensure that the information taken in the data breach at Kimpton Hotels has not been  
20 used to steal his identity or otherwise cause damage to his credit and finances. He also has  
21 taken time out of his day to review and address the alerts that he receives from the identity theft  
22 protection service to determine why he received the alerts and to take whatever action is  
23 necessary to deal with the alerts, a practice which will continue into the future . As a result of  
24 this breach, he will to continue to secure and maintain identity theft protection on a continuing  
25 basis to monitor his credit and finances.  
26  
27

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

1 **B. Kimpton and Its Private Information Collection Practices**

2 14. Kimpton primarily derives its revenues from hotel restaurant operations.

3  
4 **C. Consumers Rely On Kimpton's Private Information Security Practices**

5 15. Kimpton maintains a privacy policy available on its website:

6 Kimpton Hotel & Restaurant Group and its affiliates, including Six Continents  
7 Hotels, Inc., an InterContinental Hotels Group company, use your personal  
8 information in order to fulfill our commitment to providing an unparalleled guest  
9 service experience. As part of that undertaking, we are committed to safeguarding  
10 the privacy of the personal information that we gather.

11 As one of our guests, you understand and agree that we collect, use and disclose  
12 your personal information in accordance with this Privacy Policy for Guests (this  
13 "Policy").

14 **Types of Personal Information We Collect**

15 The term "personal information" in this Policy refers to information which does or  
16 is capable of identifying you as an individual. The types of personal information  
17 that we process (which may vary by jurisdiction based on applicable law) include:

- 18 · your name, gender, home and work contact details, business title, date and place  
19 of birth, nationality and passport and visa information;
- 20 · guest stay information, including the hotels where you have stayed, date of  
21 arrival and departure, goods and services purchased, special requests made,  
22 observations about your service preferences (including room and holiday  
23 preferences), telephone numbers dialed and faxes and telephone messages  
24 received;
- 25 · your credit card details, Kimpton Karma Rewards member information, online  
26  
27

1 user account details, profile or password details and any frequent flyer or travel  
2 partner program affiliation;

3 · any information necessary to fulfill special requests (e.g., health conditions that  
4 require specific accommodation, purchase of goods and services);

5 · information you provide regarding your marketing preferences or in the course  
6 of participating in surveys, contests or promotional offers;

7 · information collected through the use of closed circuit television systems, card  
8 key and other security systems; and

9 · contact and other relevant details concerning the employees of corporate  
10 accounts and vendors and other individuals with whom we do business (e.g.,  
11 travel agents or meeting and event planners).

12 · geolocation information for our mobile internet and iPhone app users, upon your  
13 consent

14 Most of the personal information we process is information that you or someone  
15 acting on your behalf knowingly provides to us. However, in some instances, we  
16 process personal information that we are able to infer about you based on other  
17 information you provide to us or on our interactions with you, or personal  
18 information about you that we receive from a third party.

#### 19 How We Use Information

20 Demographic and profile data is collected at our site, and we use this data in two  
21 main ways:

22 First, we analyze visitor information in aggregate, which means that we collect  
23 information about thousands of site visits and analyze it as a whole. This kind of  
24 study involves looking for trends among many visitors to our site, rather than  
25 analyzing information about any individual visitor. Examples include researching  
26  
27



1 which parts of the site are accessed most frequently or determining which  
2 products are most attractive to our users.

3 Second, we may use specific information you provide to help us customize our  
4 communications with you and improve our service to you when you visit any  
5 Kimpton property, to conduct market research, customer satisfaction and quality  
6 assurance surveys and to direct marketing and sales promotions. For instance, if  
7 you inform us of a room or service preference, we will attempt to satisfy that  
8 request when you visit us in the future and may send you promotions relating to  
9 that preference.

10 We use third parties to build and manage these communication and preference  
11 systems, and our arrangements with these third parties prohibit them from  
12 disclosing your personal information.

13 Specifically, subject to applicable laws, we may collect, use and disclose relevant  
14 portions of your personal information in order to:

- 15 · provide and charge for the hotel accommodation and other goods and services  
16 you purchase;
  - 17 · provide you with a better, more personalized level of service;
  - 18 · administer the Kimpton Karma rewards program;
  - 19 · fulfill contractual obligations to you, anyone involved in the process of making  
20 your travel arrangements (e.g., travel agents, group travel organizers or your  
21 employer) and vendors (e.g., credit card companies, airline operators and other  
22 loyalty programs);
  - 23 · conduct market research, customer satisfaction and quality assurance surveys,  
24 direct marketing and sales promotions;
  - 25 · respond to requests for information and services;
- 26  
27

- provide for the safety and security of staff, guests and other visitors;
- administer general record keeping; and
- meet legal and regulatory requirements

#### Sharing of Personal Information

We reveal Personally Identifiable Information about you to unaffiliated third parties if:

- you request or authorize it;
- the information is provided to help complete a transaction for you;
- the information is provided to comply with the law, applicable regulations, court orders or subpoenas, to enforce our Terms of Use or other agreements, or to protect our rights, property or safety or the rights, property or safety of our users or others (e.g., to a consumer reporting agency for fraud protection etc.);
- the disclosure is done as part of a changeover in management of a hotel or restaurant from Kimpton to a third party;
- the information is provided to our agents, outside vendors or service providers to perform functions on our behalf (e.g., analyzing data, providing marketing assistance, providing customer service, processing orders, etc.); or
- to others as described in this Privacy Policy.

16. Kimpton stores massive amounts of PII and PCD on its servers and utilizes this information to maximize its profits through predictive marketing and other marketing techniques.

17. Consumers place value in data privacy and security, and they consider it when making decisions on where to stay for travel. Plaintiff would not have stayed at the Kimpton hotels nor would he have used his debit card to pay for his Kimpton stays had he known that Kimpton does not take all necessary precautions to secure the personal and financial data given

1 to it by consumers.

2 18. Kimpton failed to disclose its negligent and insufficient data security practices  
3 and consumers relied on or were misled by this omission into paying, or paying more, for  
4 accommodations at Kimpton.

5  
6 **D. Stolen Private Information Is Valuable to Hackers and Thieves**

7 19. It is well known and the subject of many media reports that PII data is highly  
8 coveted and a frequent target of hackers. PII data is often easily taken because it may be less  
9 protected and regulated than payment card data. In the hospitality industry, and as identified  
10 earlier, a large number of hotel chains were the targets of data breaches. Moreover, Kimpton—  
11 along with the other hotel chains that were hacked—was aware or should have been aware of  
12 the federal government’s heightened interest in securing consumers’ PII when staying in hotels  
13 located in the United States due to the very public litigation commenced by the Federal Trade  
14 Commission against Wyndham Worldwide Corporation founded upon that company’s failure  
15 to provide reasonable cybersecurity protections for customer data. Despite this well-publicized  
16 litigation and the frequent public announcements of data breaches by retailers and hotel chains,  
17 Kimpton opted to maintain an insufficient and inadequate system to protect the PII of Plaintiff  
18 and class members.

19 20. Legitimate organizations and the criminal underground alike recognize the value  
20 of PII. Otherwise, they wouldn’t aggressively seek or pay for it. For example, in “one of 2013’s  
21 largest breaches . . . not only did hackers compromise the [card holder data] of three million  
22 customers, they also took registration data from 38 million users.”<sup>1</sup> Similarly, in the Target data  
23 breach, in addition to PCI data pertaining to 40,000 credit and debit cards, hackers stole PII

24  
25 <sup>1</sup> Verizon 2014 PCI Compliance Report, available at [http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon\\_pci-report-2014.pdf](http://www.nocash.info.ro/wp-content/uploads/2014/02/Verizon_pci-report-2014.pdf) (hereafter “2014 Verizon Report”), at  
26 54 (last visited Sept. 24, 2014).  
27

1 pertaining to 70,000 customers.

2 21. Biographical data is also highly sought after by data thieves. “Increasingly,  
3 criminals are using biographical data gained from multiple sources to perpetrate more and  
4 larger thefts.” *Id.* PII data has been stolen and sold by the criminal underground on many  
5 occasions in the past, and the accounts of theft and unauthorized access have been the subject  
6 of many media reports. One form of identity theft, branded “synthetic identity theft,” occurs  
7 when thieves create new identities by combining real and fake identifying information then use  
8 those identities to open new accounts. “This is where they’ll take your Social Security number,  
9 my name and address, someone else’s birthday and they will combine them into the equivalent  
10 of a bionic person,” said Adam Levin, Chairman of IDT911, which helps businesses recover  
11 from identity theft. Synthetic identity theft is harder to unravel than traditional identity theft,  
12 experts said: “It’s tougher than even the toughest identity theft cases to deal with because they  
13 can’t necessarily peg it to any one person.” In fact, the fraud might not be discovered until an  
14 account goes to collections and a collection agency researches the Social Security number.

15 22. Unfortunately, and as is alleged below, despite all of this publicly available  
16 knowledge of the continued compromises of PII in the hands of third parties, such as hoteliers ,  
17 Kimpton’s approach at maintaining the privacy of Plaintiff’s and Class members’ PII was  
18 lackadaisical, cavalier, reckless, or at the very least, negligent.

19 **E. Kimpton Failed to Segregate PCD From PII**

20 23. Unlike PII data, PCD is heavily regulated. The Payment Card Industry Data  
21 Security Standard (“PCI DSS”) is a set of requirements designed to ensure that companies  
22 maintain consumer credit and debit card information in a secure environment.

23 24. “PCI DSS provides a baseline of technical and operational requirements  
24  
25  
26  
27

1 designed to protect cardholder data.”<sup>2</sup>

2 25. One PCI DSS requirement is to protect stored cardholder data. Cardholder data  
3 includes Primary Account Number, Cardholder Name, Expiration Date, and Service Code.  
4 “Network segmentation of, or isolating (segmenting), the cardholder data environment from the  
5 remainder of an entity’s network is not a PCI DSS requirement.”<sup>3</sup> However, segregation is  
6 recommended because, among other reasons, “[i]t’s not just cardholder data that’s important;  
7 criminals are also after personally identifiable information (PII) and corporate data.”<sup>4</sup>

8 26. Illicitly obtained PII and PCD, sometimes aggregated from different data  
9 breaches, are sold on the black market, including on websites, as products at a set price.<sup>5</sup>

10 27. Without such detailed disclosure, Plaintiff and Class members are unable to take  
11 the necessary precautions to prevent imminent harm, such as continued misuse of their personal  
12 information.

13 28. Kimpton has failed to provide a cogent picture of how the Data Breach occurred  
14 and its full effects on consumers’ PII and PCD information.

15 29. Hacking is often accomplished in a series of phases, including reconnaissance;  
16 scanning for vulnerabilities and enumeration of the network; gaining access; escalation of user,  
17 computer and network privileges; maintaining access; covering tracks; and placing backdoors.  
18 On information and belief, while hackers scoured Kimpton’s networks to find a way to access  
19 PCD, they had access to and collected the PII stored on Kimpton’s networks.

20 30. Thieves already are using the Private Information stolen from Kimpton to  
21

---

22 <sup>2</sup> PCI SECURITY STANDARDS COUNCIL, PAYMENT CARD INDUSTRY DATA SECURITY STANDARD  
23 VERSION 2.0 at 5 (October 2010) (hereafter PCI Version 2).

24 <sup>3</sup> *Id.* at 10.

25 <sup>4</sup> See Verizon Report at 54.

26 <sup>5</sup> See, e.g., Brian Krebs, *How Much Is Your Identity Worth?*, KREBSONSECURITY.COM (Nov. 8,  
27 2011), <https://krebsonsecurity.com/2011/11/how-much-is-your-identity-worth/> (last visited  
January 18, 2016).

1 commit actual fraud, as occurred to Plaintiff here.

2 31. The Data Breach was caused and enabled by Kimpton's knowing violation of its  
3 obligations to abide by best practices and industry standards in protecting its customers' Private  
4 Information.

5 32. In this regard, more than likely the software used in the attack was a variant of  
6 "BlackPOS," a malware strain designed to siphon data from cards when they are swiped at  
7 infected point-of-sale systems. Hackers previously utilized BlackPOS in other recent cyber-  
8 attacks, including breaches at Home Depot and Target. While many retailers, banks, and card  
9 companies have responded to these recent breaches by adopting technology and security  
10 practices that help makes transactions and stored data more secure, Kimpton has acknowledged  
11 that it did not do so.

12 **F. This Data Breach Will Result In Additional Identity Theft and Identify Fraud**

13 33. Kimpton failed to implement and maintain reasonable security procedures and  
14 practices appropriate to the nature and scope of the Private Information compromised in the  
15 Data Breach.

16 34. The ramifications of Kimpton's failure to keep Plaintiff's and Class members'  
17 data secure are severe.

18 35. The information Kimpton compromised, including Plaintiff's identifying  
19 information and/or other financial information, is "as good as gold" to identity thieves, in the  
20 words of the Federal Trade Commission ("FTC").<sup>6</sup> Identity theft occurs when someone uses  
21 another's personal identifying information, such as that person's name, address, credit card  
22 number, credit card expiration date, and other information, without permission, to commit fraud  
23 or other crimes. The FTC estimates that as many as 10 million Americans have their identities

24 <sup>6</sup> FTC Interactive Toolkit, Fighting Back Against Identity Theft, *available at*  
25 <http://www.dcsheiff.net/community/documents/id-theft-tool-kit.pdf> (last visited Sept. 24,  
26 2014).

1 stolen each year.

2 36. As the FTC recognizes, once identity thieves have personal information, “they  
3 can drain your bank account [as occurred to Plaintiff here], run up your credit cards, open new  
4 utility accounts, or get medical treatment on your health insurance.”<sup>7</sup>

5 37. According to Javelin Strategy and Research, “1 in 4 notification recipients  
6 became a victim of identity fraud.”<sup>8</sup> Nearly half (46%) of consumers with a breached debit card  
7 became fraud victims within the same year.

8 38. Identity thieves can use personal information such as that of Plaintiff and Class  
9 members, which Kimpton failed to keep secure, to perpetrate a variety of crimes that harm  
10 victims. For instance, identity thieves may commit various types of government fraud such as:  
11 immigration fraud; obtaining a driver’s license or identification card in the victim’s name but  
12 with another’s picture; using the victim’s information to obtain government benefits; or filing a  
13 fraudulent tax return using the victim’s information to obtain a fraudulent refund. Some of this  
14 activity may not come to light for years. The IRS paid out 43.6 billion in potentially fraudulent  
15 returns in 2012, and the IRS identified more than 2.9 million incidents of identity theft in 2013.  
16 The IRS has described identity theft as the number one tax scam for 2014.

17 39. Among other forms of fraud, identity thieves may get medical services using  
18 consumers’ compromised personal information or commit any number of other frauds, such as  
19 obtaining a job, procuring housing, or even giving false information to police during an arrest.

20 40. It is incorrect to assume that reimbursing a consumer for a financial loss due to  
21 fraud makes that individual whole again. On the contrary, after conducting a study, the  
22

---

23 <sup>7</sup> FTC, Signs of Identity Theft, available at <<http://www.consumer.ftc.gov/articles/0271-signs-identity-theft>> (last visited Sept. 24, 2014).

24 <sup>8</sup> See 2013 Identity Fraud Report: Data Breaches Becoming a Treasure Trove for Fraudsters,  
25 available at <[www.javelinstrategy.com/brochure/276](http://www.javelinstrategy.com/brochure/276)> (last visited Sept. 24, 2014) (the “2013  
26 Identity Fraud Report”).  
27

1 Department of Justice’s Bureau of Justice Statistics (“BJS”) found that “among victims who  
2 had personal information used for fraudulent purposes, 29% spent a month or more resolving  
3 problems.”<sup>9</sup> In fact, the BJS reported, “resolving the problems caused by identity theft [could]  
4 take more than a year for some victims.” *Id.* at 11.

5 **G. Annual monetary losses from identity theft are in the billions of dollars.**

6 41. Javelin Strategy and Research reports that those losses increased to \$21 billion  
7 in 2013.<sup>10</sup>

8 42. There may be a time lag between when harm occurs versus when it is  
9 discovered, and also between when PII or PCD is stolen and when it is used. According to the  
10 U.S. Government Accountability Office (“GAO”), which conducted a study regarding data  
11 breaches:

12 [L]aw enforcement officials told us that in some cases, stolen data may be held  
13 for up to a year or more before being used to commit identity theft. Further,  
14 once stolen data have been sold or posted on the Web, fraudulent use of that  
15 information may continue for years. As a result, studies that attempt to measure  
the harm resulting from data breaches cannot necessarily rule out all future  
harm.<sup>11</sup>

16 43. Plaintiff and Class members now face years of constant surveillance of their  
17 financial and personal records, monitoring, and loss of rights. The Class is incurring and will  
18 continue to incur such damages in addition to any fraudulent credit and debit card charges  
19 incurred by them and the resulting loss of use of their credit and access to funds, whether or not  
20 such charges are ultimately reimbursed by the credit card companies.

21 **H. Plaintiff and Class Members Suffered Damages**

22 44. The Data Breach was a direct and proximate result of Kimpton’s failure to

23 <sup>9</sup> Victims of Identity Theft, 2012 (Dec. 2013) at 10, available at  
24 <http://www.bjs.gov/content/pub/pdf/vit12.pdf> (last visited Sept. 24, 2014).

25 <sup>10</sup> See 2013 Identity Fraud Report.

26 <sup>11</sup> GAO, Report to Congressional Requesters, at p.33 (June 2007), available at  
27 <http://www.gao.gov/new.items/d07737.pdf> (emphases added) (last visited Sept. 24, 2014).



1 properly safeguard and protect Plaintiff's and Class members' Private Information from  
2 unauthorized access, use, and disclosure, as required by various state and federal regulations,  
3 industry practices, and the common law, including Kimpton's failure to establish and  
4 implement appropriate administrative, technical, and physical safeguards to ensure the security  
5 and confidentiality of Plaintiff's and Class members' PII to protect against reasonably  
6 foreseeable threats to the security or integrity of such information.

7 45. Plaintiff's and Class members' PII is private and sensitive in nature and was left  
8 inadequately protected by Kimpton. Kimpton did not obtain Plaintiff's and Class members'  
9 consent to disclose their PII to any other person as required by applicable law and industry  
10 standards.

11 46. As a direct and proximate result of Kimpton's wrongful action and inaction and  
12 the resulting Data Breach, Plaintiff (as was addressed above) and Class members have been  
13 placed at an imminent, immediate, and continuing increased risk of harm from identity theft  
14 and identity fraud, requiring them to take the time and effort to mitigate the actual and potential  
15 impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts"  
16 with credit reporting agencies, contacting their financial institutions, closing or modifying  
17 financial accounts, and closely reviewing and monitoring their credit reports and accounts for  
18 unauthorized activity.

19 47. Kimpton's wrongful actions and inaction directly and proximately caused the  
20 theft and dissemination into the public domain of Plaintiff's and Class members' Private  
21 Information, causing them to suffer, and continue to suffer, economic damages and other actual  
22 harm for which they are entitled to compensation, including:

- 23 a. theft of their personal and financial information;
- 24 b. the imminent and certainly impending injury flowing from potential fraud  
25 and identity theft posed by their credit/debit card and personal information  
26  
27

1 being placed in the hands of criminals and already misused via the sale of  
2 Plaintiff's and Class members' information on the Internet card black  
3 market;

4 c. the untimely and inadequate notification of the Data Breach;

5 d. the improper disclosure of their Private Information;

6 e. loss of privacy;

7 f. ascertainable losses in the form of out-of-pocket expenses and the value of  
8 their time reasonably incurred to remedy or mitigate the effects of the Data  
9 Breach;

10 g. ascertainable losses in the form of deprivation of the value of their PII and  
11 PCD, for which there is a well-established national and international market;

12 h. overpayments to Kimpton for products and services purchased during the  
13 Data Breach in that a portion of the price paid for such products and services  
14 by Plaintiffs and Class members to Kimpton was for the costs of reasonable  
15 and adequate safeguards and security measures that would protect  
16 customers' Private Information, which Kimpton did not implement and, as a  
17 result, Plaintiff and Class members did not receive what they paid for and  
18 were overcharged by Kimpton;

19 i. the loss of use of and access to their account funds and costs associated with  
20 inability to obtain money from their accounts or being limited in the amount  
21 of money they were permitted to obtain from their accounts; and

22 j. deprivation of rights they possess under the California Unfair Competition  
23 Law (Cal. Bus. & Prof. Code §17200);

24 k. Plaintiff's economic injury is also described in Paragraph 7.

25 48. While the Private Information of Plaintiff and members of the Class has been  
26  
27

1 stolen, the same or a copy of the Private Information continues to be held by Kimpton. Plaintiff  
2 and members of the Class have an undeniable interest in insuring that this information is  
3 secure, remains secure, and is not subject to further theft.

#### 4 **CLASS ACTION ALLEGATIONS**

5 49. Plaintiff seeks relief in her individual capacity and as representatives of all  
6 others who are similarly situated. Pursuant to Fed. R. Civ. P. 23(a) and (b)(2), (b)(3), and  
7 (c)(4), Plaintiff seeks certification of a Nationwide class and a California class. The national  
8 class is initially defined as follows: all persons residing in the United States whose personal  
9 and/or financial information was disclosed in the Data Breach affecting Kimpton in 2015 (the  
10 “Nationwide Class”).

11 50. The California Class is initially defined as follows: all persons residing in  
12 California whose personal and/or financial information was disclosed in the Data Breach  
13 affecting Kimpton in 2016 (the “California Class”).

14 51. Excluded from each of the above Classes are Kimpton, including any entity in  
15 which Kimpton has a controlling interest, is a parent or subsidiary, or which is controlled by  
16 Kimpton, as well as the officers, directors, affiliates, legal representatives, heirs, predecessors,  
17 successors, and assigns of Kimpton. Also excluded are the judges and court personnel in this  
18 case and any members of their immediate families.

19 52. Numerosity. Fed. R. Civ. P. 23(a)(1). The members of the Class are so  
20 numerous that the joinder of all members is impractical. While the exact number of Class  
21 members is unknown to Plaintiff at this time, Kimpton has acknowledged that debit and credit  
22 cards were affected by the breach at many of its hotels in the United States, including the one  
23 where Plaintiff stayed.

24 53. Commonality. Fed. R. Civ. P. 23(a)(2) and (b)(3). There are questions of law  
25 and fact common to the Class, which predominate over any questions affecting only individual  
26  
27

1 Class members. These common questions of law and fact include, without limitation:

- 2 a. Whether Kimpton violated the California’s Deceptive and Unfair Trade  
3 Practices Act by failing to implement reasonable security procedures and  
4 practices;
- 5 b. Whether Kimpton violated law by failing to promptly notify class members  
6 their personal information had been compromised;
- 7 c. Whether class members may obtain injunctive relief against Kimpton under  
8 California’s privacy laws to require that it safeguard or destroy, rather than  
9 retain, the Private Information of Plaintiff and Class members;
- 10 d. Which security procedures and which data-breach notification procedure  
11 should Kimpton be required to implement as part of any injunctive relief  
12 ordered by the Court;
- 13 e. Whether Kimpton has an implied contractual obligation to use reasonable  
14 security measures;
- 15 f. Whether Kimpton has complied with any implied contractual obligation to  
16 use reasonable security measures;
- 17 g. What security measures, if any, must be implemented by Kimpton to comply  
18 with its implied contractual obligations;
- 19 h. Whether Kimpton violated California’s privacy laws in connection with the  
20 actions described herein; and
- 21 i. What the nature of the relief should be, including equitable relief, to which  
22 Plaintiff and the Class members are entitled.

23 54. All members of the proposed Classes are readily ascertainable. Kimpton has  
24 access to addresses and other contact information for millions of members of the Classes,  
25 which can be used for providing notice to many Class members.  
26  
27



1 and make purchases using their credit or debit cards. Plaintiff and Class members accepted  
2 Kimpton's offers and used their credit or debit cards to purchase, stay, and make purchases at  
3 Kimpton hotels during the period of the Data Breach.

4         62. When Plaintiff and Class Members made and paid for purchases of Kimpton  
5 services and products in connection with their stays at Kimpton properties, they provided their  
6 PII and PCD, including but not limited to the PII and PCD contained on the face of, and  
7 embedded in the magnetic strip of, their debit and credit cards. In so doing, Plaintiff and Class  
8 Members entered into implied contracts with Kimpton pursuant to which Kimpton agreed to  
9 safeguard and protect such information and to timely and accurately notify Plaintiff and Class  
10 Members if their data had been breached and compromised.

11         63. Each purchase at a Kimpton hotel made by Plaintiff and Class Members using  
12 their credit or debit card was made pursuant to the mutually agreed-upon implied contract with  
13 Kimpton under which Kimpton agreed to safeguard and protect Plaintiff's and Class Members'  
14 PII and PCD, including all information contained in the magnetic stripe of Plaintiff's and Class  
15 Members' credit or debit cards, and to timely and accurately notify them if such information  
16 was compromised or stolen.

17         64. Plaintiff and Class Members would not have provided and entrusted their PII  
18 and PCD, including all information contained in the magnetic stripes of their credit and debit  
19 cards, to Kimpton to stay at its hotels and make purchases in the absence of the implied  
20 contract between them and Kimpton.

21         65. Plaintiff and Class Members fully performed their obligations under the implied  
22 contracts with Kimpton.

23         66. Kimpton breached the implied contracts it made with Plaintiff and Class  
24 Members by failing to safeguard and protect the PII and PCD of Plaintiff and Class Members  
25 and by failing to provide timely and accurate notice to them that their PII and PCD was  
26  
27

1 compromised in and as a result of the Data Breach.

2 67. As a direct and proximate result of Kimpton's breaches of the implied contracts  
3 between Kimpton and Plaintiff and Class Members, Plaintiff and Class Members sustained  
4 actual losses and damages as described in detail above.

5 **COUNT II**

6 **Negligence**

7 (On Behalf of Plaintiff and the Nationwide Class)

8 68. Plaintiff incorporates the substantive allegations contained in Paragraphs 1  
9 through 59 as if fully set forth herein.

10 69. Upon accepting and storing Plaintiff's and Class Members' Private Information  
11 in their respective computer database systems, Kimpton undertook and owed a duty to Plaintiff  
12 and Class Members to exercise reasonable care to secure and safeguard that information and to  
13 utilize commercially reasonable methods to do so. Kimpton knew, acknowledged, and agreed  
14 the Private Information was private and confidential and would be protected as private and  
15 confidential.

16 70. The law imposes an affirmative duty on Kimpton to timely disclose the  
17 unauthorized access and theft of the Private Information to Plaintiff and the Class so that  
18 Plaintiff and Class Members could take appropriate measures to mitigate damages, protect  
19 against adverse consequences, and thwart future misuse of their Private Information.

20 71. Kimpton breached its duty to notify Plaintiff and Class Members of the  
21 unauthorized access by failing to notify Plaintiff and Class Members of the breach until  
22 September 2016. To date, Kimpton has not provided sufficient information to Plaintiff and  
23 Class Members regarding the extent of the unauthorized access and continues to breach its  
24 disclosure obligations to Plaintiff and the Class.

25 72. Kimpton also breached its duty to Plaintiff and the Class Members to adequately  
26  
27

1 protect and safeguard this information by knowingly disregarding standard information security  
2 principles, despite obvious risks, and by allowing unmonitored and unrestricted access to  
3 unsecured Private Information. Furthering its dilatory practices, Kimpton failed to provide  
4 adequate supervision and oversight of the Private Information with which it is entrusted, in  
5 spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a  
6 third party to gather Plaintiff's and Class Members' Private Information, misuse the Private  
7 Information, and intentionally disclose it to others without consent.

8         73. Through Kimpton's acts and omissions described in this Complaint, including  
9 Kimpton's failure to provide adequate security and its failure to protect Plaintiff's and Class  
10 Members' Private Information from being foreseeably captured, accessed, disseminated, stolen,  
11 and misused, Kimpton unlawfully breached its duty to use reasonable care to adequately protect  
12 and secure Plaintiff's and Class Members' Private Information during the time it was within  
13 Kimpton's possession or control.

14         74. Further, through its failure to provide timely and clear notification of the Data  
15 Breach to consumers, Kimpton prevented Plaintiff and Class Members from taking meaningful,  
16 proactive steps to secure their financial data and bank accounts.

17         75. Upon information and belief, Kimpton improperly and inadequately safeguarded  
18 the Private Information of Plaintiff and Class Members in deviation from standard industry  
19 rules, regulations, and practices at the time of the Data Breach.

20         76. Kimpton's failure to take proper security measures to protect Plaintiff's and  
21 Class Members' sensitive Private Information as described in this Complaint, created  
22 conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access  
23 of Plaintiff's and Class Members' Private Information.

24         77. Kimpton's conduct was grossly negligent and departed from all reasonable  
25  
26  
27



1 standards of care, including, but not limited to: failing to adequately protect the Private  
2 Information; failing to conduct regular security audits; failing to provide adequate and  
3 appropriate supervision of persons having access to Plaintiff's and Class Members' Private  
4 Information; and failing to provide Plaintiff and Class Members with timely and sufficient  
5 notice that their sensitive Private Information had been compromised.

6 78. Neither Plaintiff nor the other Class Members contributed to the Data Breach  
7 and subsequent misuse of their Private Information as described in this Complaint.

8 79. As a direct and proximate cause of Kimpton's conduct, Plaintiff and the Class  
9 suffered damages including, but not limited to: damages arising from the unauthorized charges  
10 on their debit or credit cards or on cards that were fraudulently obtained through the use of the  
11 Private Information of Plaintiff and Class Members and/or filing false tax returns; and damages  
12 from identity theft, which may take months, if not years, to discover and detect, given the far-  
13 reaching, adverse, and detrimental consequences of identity theft and loss of privacy. The  
14 nature of other forms of economic damage and injury may take years to detect and the potential  
15 scope can only be assessed after a thorough investigation of the facts and events surrounding  
16 the theft mentioned above.

### 17 **COUNT III**

#### 18 **Violation of California's Unfair Competition Law** 19 **Cal. Bus. & Prof. Code §17200 – Unlawful Business Practices** 20 (On Behalf of the California Class)

21 80. Plaintiff incorporates the substantive allegations contained in Paragraphs 1  
22 through 59 as if fully set forth herein.

23 81. Kimpton has violated Cal. Bus. and Prof. Code §17200 et seq. by engaging in  
24 unlawful, unfair or fraudulent business acts and practices and unfair, deceptive, untrue or  
25 misleading advertising that constitute acts of "unfair competition" as defined in Cal. Bus. Prof.  
26 Code §17200 with respect to the hotel services provided to the California Class.  
27

1           82.     Kimpton engaged in unlawful acts and practices with respect to the hotel  
2 services by establishing the sub-standard security practices and procedures described herein; by  
3 soliciting and collecting Plaintiff's and California Class Members' Private Information with  
4 knowledge that the information would not be adequately protected; and by storing Plaintiff's  
5 and California Class Members' Private Information in an unsecure electronic environment in  
6 violation of California's data breach statute, Cal. Civ. Code § 1798.81.5, which requires  
7 Kimpton to take reasonable methods of safeguarding the Private Information of Plaintiff and  
8 the California Class Members.

9           83.     In addition, Kimpton engaged in unlawful acts and practices with respect to the  
10 sale of hotel services by failing to disclose the Data Breach to California Class Members in a  
11 timely and accurate manner, contrary to the duties imposed by Cal. Civ. Code § 1798.82. To  
12 date, Kimpton has still not provided such information to Plaintiff and the California Class  
13 Members.

14           84.     As a direct and proximate result of Kimpton's unlawful practices and acts,  
15 Plaintiff and the California Class Members were injured and lost money or property, including  
16 but not limited to the price received by Kimpton for the hotel services, the loss of their legally  
17 protected interest in the confidentiality and privacy of their Private Information, and additional  
18 losses described above.

19           85.     Kimpton knew or should have known that its computer systems and data  
20 security practices were inadequate to safeguard California Class Members' Private Information  
21 and that the risk of a data breach or theft was highly likely. Kimpton's actions in engaging in  
22 the above-named unlawful practices and acts were negligent, knowing and willful, and/or  
23 wanton and reckless with respect to the rights of members of the California Class.  
24

25           86.     California Class Members seek relief under Cal. Bus. & Prof. Code § 17200, et.  
26  
27

1 seq., including, but not limited to, restitution to Plaintiff and California Class Members of  
2 money or property that Kimpton may have acquired by means of its unlawful, and unfair  
3 business practices, restitutionary disgorgement of all profits accruing to Kimpton because of its  
4 unlawful and unfair business practices, declaratory relief, attorney's fees and costs (pursuant to  
5 Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

6 **COUNT IV**  
7 **Violation of California's Unfair Competition Law**  
8 **Cal. Bus. & Prof. Code §17200 – Unfair Business Practices**  
9 (On Behalf of the California Class)

10 87. Plaintiff incorporates the substantive allegations contained in Paragraphs 1  
11 through 59 as if fully set forth herein.

12 88. Kimpton engaged in unfair acts and practices with respect to the hotel services  
13 by establishing the sub-standard security practices and procedures described herein; by  
14 soliciting and collecting Plaintiff's and California Class Members' Private Information with  
15 knowledge that the information would not be adequately protected; and by storing Plaintiff's  
16 and California Class Members' Private Information in an unsecure electronic environment.  
17 These unfair acts and practices were immoral, unethical, oppressive, unscrupulous,  
18 unconscionable, and/or substantially injurious to Plaintiffs and California Class Members.  
19 They were likely to deceive the public into believing their Private Information was securely  
20 stored, when it was not. The harm these practices caused to Plaintiffs and the California Class  
21 Members outweighed their utility, if any.

22 89. Kimpton engaged in unfair acts and practices with respect to the provision of  
23 hotel services by failing to take proper action following the Data Breach to enact adequate  
24 privacy and security measures and protect California Class Members' Private Information from  
25 further unauthorized disclosure, release, data breaches, and theft. These unfair acts and  
26 practices were immoral, unethical, oppressive, unscrupulous, unconscionable, and/or  
27

1 substantially injurious to Plaintiff and California Class Members. They were likely to deceive  
2 the public into believing their Private Information was securely stored, when it was not. The  
3 harm these practices caused to Plaintiff and the California Class Members outweighed their  
4 utility, if any.

5 90. As a direct and proximate result of Kimpton's acts of unfair practices and acts,  
6 Plaintiff and the California Class Members were injured and lost money or property, including  
7 but not limited to the price received by Kimpton for the hotel services, the loss of their legally  
8 protected interest in the confidentiality and privacy of their Private Information, and additional  
9 losses described above.

10 91. Kimpton knew or should have known that its computer systems and data  
11 security practices were inadequate to safeguard California Class Members' Private Information  
12 and that the risk of a data breach or theft was highly likely. Kimpton's actions in engaging in  
13 the above-named unlawful practices and acts were negligent, knowing and willful, and/or  
14 wanton and reckless with respect to the rights of members of the California Class.

15 92. California Class Members seek relief under Cal. Bus. & Prof. Code § 17200, et.  
16 seq., including, but not limited to, restitution to Plaintiff and California Class Members of  
17 money or property that the Kimpton may have acquired by means of its unfair business  
18 practices, restitutionary disgorgement of all profits accruing to Kimpton because of its unfair  
19 business practices, declaratory relief, attorney's fees and costs (pursuant to Cal. Code Civ.  
20 Proc. §1021.5), and injunctive or other equitable relief.

21  
22 **COUNT IV**

23 **Violation of California's Unfair Competition Law**  
24 **Cal. Bus. & Prof. Code §17200 – Fraudulent/Deceptive Business Practices**  
25 **(On Behalf of the California Class)**

26 93. Plaintiff incorporates the substantive allegations contained in Paragraphs 1  
27 through 59 as if fully set forth herein.

1           94.     Kimpton engaged in fraudulent and deceptive acts and practices with regard to  
2 the hotel services provided to the California Class by representing and advertising that it would  
3 maintain adequate data privacy and security practices and procedures to safeguard California  
4 Class Members' Private Information from unauthorized disclosure, release, data breaches, and  
5 theft; and representing and advertising that it did and would comply with the requirements of  
6 relevant federal and state laws pertaining to the privacy and security of California Class  
7 Members' Private Information. These representations were likely to deceive members of the  
8 public, including Plaintiff and the California Class Members, into believing their Private  
9 Information was securely stored, when it was not, and that Kimpton was complying with  
10 relevant law, when it was not.

11           95.     Kimpton engaged in fraudulent and deceptive acts and practices with regard to  
12 the hotel services provided to the California Class by omitting, suppressing, and concealing the  
13 material fact of the inadequacy of the privacy and security protections for California Class  
14 Members' Private Information. At the time that California Class members were using  
15 Kimpton's hotel services, Kimpton failed to disclose to California Class Members that its data  
16 security systems failed to meet legal and industry standards for the protection of their Private  
17 Information. Plaintiffs would not have selected Kimpton to provide hotel services if they had  
18 known about its substandard data security practices. These representations were likely to  
19 deceive members of the public, including Plaintiff and the California Class Members, into  
20 believing their Private Information was securely stored, when it was not, and that Kimpton was  
21 complying with relevant law and industry standards, when it was not.

22           96.     As a direct and proximate result of Kimpton's deceptive practices and acts,  
23 Plaintiff and the California Class Members were injured and lost money or property, including  
24 but not limited to the price received by Kimpton for the hotel services, the loss of their legally  
25 protected interest in the confidentiality and privacy of their Private Information, and additional  
26  
27

1 losses described above.

2 97. Kimpton knew or should have known that its computer systems and data  
3 security practices were inadequate to safeguard California Class Members' Private Information  
4 and that the risk of a data breach or theft was highly likely. Kimpton's actions in engaging in  
5 the above-named unlawful practices and acts were negligent, knowing and willful, and/or  
6 wanton and reckless with respect to the rights of members of the California Class.

7 98. California Class Members seek relief under Cal. Bus. & Prof. Code § 17200, et.  
8 seq., including, but not limited to, restitution to Plaintiff and California Class Members of  
9 money or property that the Kimpton may have acquired by means of its fraudulent and  
10 deceptive business practices, restitutionary disgorgement of all profits accruing to Kimpton  
11 because of its fraudulent and deceptive business practices, declaratory relief, attorney's fees  
12 and costs (pursuant to Cal. Code Civ. Proc. §1021.5), and injunctive or other equitable relief.

### 13 **REQUEST FOR RELIEF**

14 **WHEREFORE**, Plaintiff, individually and on behalf of all Class members proposed in  
15 this Complaint, respectfully requests that the Court enter judgment in her favor and against  
16 Kimpton as follows:

- 17 a. For an Order certifying the Nationwide Class and California Class as  
18 defined herein, and appointing Plaintiff and his Counsel to represent the  
19 Nationwide Class and California Class;
- 20 b. For equitable relief enjoining Kimpton from engaging in the wrongful  
21 conduct complained of herein pertaining to the misuse and/or disclosure of  
22 Plaintiff and Class members' Private Information, and from refusing to issue  
23 prompt, complete, and accurate disclosures to the Plaintiff and Class  
24 members;
- 25 c. For equitable relief compelling Kimpton to utilize appropriate methods and  
26  
27

1 policies with respect to consumer data collection, storage, and safety and to  
2 disclose with specificity to Class members the type of PII and PCD  
3 compromised.

- 4 d. For equitable relief requiring restitution and disgorgement of the revenues  
5 wrongfully retained as a result of Kimpton's wrongful conduct;  
6 e. For an award of actual damages and compensatory damages, in an amount to  
7 be determined;  
8 f. For an award of costs of suit and attorneys' fees, as allowable by law; and  
9 g. Such other and further relief as this court may deem just and proper.

10 **JURY TRIAL DEMAND**

11 Plaintiff demands a jury trial on all issues so triable.

12 Dated: January 6, 2017

13 Respectfully submitted,

14 **MORGAN & MORGAN COMPLEX  
15 LITIGATION GROUP**

16 By: /s/ John A. Yanchunis  
17 John A. Yanchunis [*Pro Hac Vice*]  
18 Florida Bar No. 324681  
19 Email: [jyanchunis@ForThePeople.com](mailto:jyanchunis@ForThePeople.com)  
20 Marisa A. Glassman [*Pro Hac Vice*]  
21 Florida Bar No. 111991  
22 Email: [mglassman@ForThePeople.com](mailto:mglassman@ForThePeople.com)  
23 201 N. Franklin Street, 7th Floor  
24 Tampa, Florida 33602  
25 Telephone: (813) 223-5505  
26 Facsimile: (813) 222-4793

27 Michael F. Ram, SBN #104805  
Email: [mram@rocklawcal.com](mailto:mram@rocklawcal.com)  
**RAM, OLSON, CEREGHINO &  
KOPCZYNSKI LLP**  
101 Montgomery Street, Suite 1800  
San Francisco, California 94104  
Telephone: (415) 433-4949

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

Facsimile: (415) 433-7311

*Attorneys for Plaintiff and Proposed Class and California Sub-Class*