TERESA C. CHOW, SBN 237694
tchow@bakerlaw.com
MATTHEW PEARSON, SBN 294302
mpearson@bakerlaw.com
BAKER & HOSTETLER LLP
11601 Wilshire Boulevard, Suite 1400
Los Angeles, California 90025
Telephone: 310.820.8800
Facsimile: 310.820.8859

DANIEL R. WARREN, *admitted pro hac vice*
dwarren@bakerlaw.com
DAVID A. CARNEY, *admitted pro hac vice*
dcarney@bakerlaw.com
DOUGLAS L. SHIVELY, *admitted pro hac vice*
dshively@bakerlaw.com
BAKER & HOSTETLER LLP
127 Public Square, Suite 2000
Cleveland, Ohio 44114
Telephone: 216.620.0200
Facsimile: 216.696.0740

Attorneys for Defendant
KIMPTON HOTEL & RESTAURANT GROUP, LLC

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

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

Plaintiff,

v.

KIMPTON HOTEL & RESTAURANT GROUP, LLC,

Defendant.

CASE NO. 3:16-cv-05387-VC

REPLY BRIEF IN SUPPORT OF MOTION TO DISMISS

Date: March 30, 2017
Time: 10:00 a.m.
Dept.: 4, 17th Floor
Before: Hon. Vince G. Chhabria

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

BAKER & HOSTETLER LLP
ATTORNEYS AT LAW
LOS ANGELES

INTRODUCTION

Plaintiff is now down to three purported injuries that he claims resulted from the malware attack at Kimpton: (1) "his valuable PII was stolen," (2) "he was forced to spend time monitoring his credit," and (3) "he remains at considerable risk for identity theft and fraud." (Opp. 1.)[1] None of these alleged injuries are sufficient to give him standing to sue or state a claim on the merits.

I. PLAINTIFF HAS NOT ALLEGED AN INJURY THAT CAN FAIRLY BE TRACED TO THE MALWARE ATTACK AT KIMPTON.

A. Theft of Data Alone Is Not Sufficient to Provide Standing.

Plaintiff claims to have standing based on the alleged theft of his personal data. But many data breach cases, including a Fourth Circuit case decided since Kimpton filed this motion to dismiss, have held that the mere theft of information – in the absence of some resulting harm – does *not* establish standing. *See Beck v. McDonald*, --- F.3d ----, 2017 WL 477781, at *7 (4th Cir. Feb. 6, 2017) ("the mere theft of these items, without more, cannot confer Article III standing"); *see also Dugas v. Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *5 (S.D. Cal. Nov. 3, 2016); *Duqum v. Scottrade, Inc.*, 2016 WL 3683001, at *8 (E.D. Mo. Jul. 12, 2016); *In re Zappos.com, Inc. Cust. Data Sec. Breach Litig.*, 108 F. Supp. 3d 949, 962 n.5 (D. Nev. 2015); *Storm v. Paytime, Inc.*, 90 F. Supp. 3d 359, 366 (M.D. Pa. 2015) (same). In his opposition brief, plaintiff fails to address this point, which applies with particular force where, as here, only payment card data is at issue. *See Dugas*, 2016 WL 6523428, at *5 (theft of payment card data does not qualify as "concrete harm sufficient for standing purposes").

In any event, plaintiff has not given the Court a sufficient basis to infer that his information was stolen to begin with. As Kimpton explained in its opening brief, plaintiff claims to have suffered only one unauthorized transaction, and it occurred on a payment card he used at Kimpton in December 2015, well outside the at-risk window. (Am. Compl. ¶ 12.) In his opposition brief, plaintiff does not challenge the unavoidable conclusion that this alleged

[1] In his opposition brief, plaintiff does not contend he has standing based on overpayment, deprivation of value, untimely notification, or an alleged violation of his statutory rights. He has therefore abandoned these theories of standing, none of which have merit in any event for the reasons explained in Kimpton's opening brief. (Open. Br. 7-9.)

unauthorized transaction had nothing to do with the malware attack at issue; indeed, he does not mention this alleged transaction in his opposition brief at all.

Plaintiff thus relies solely on his second visit to Kimpton, on May 29, 2016, which did fall within the at-risk window. (Am. Compl. ¶ 13; Opp. 1.) But plaintiff does not allege any misuse of the information on this payment card that would indicate it was actually stolen. Moreover, the notice on which he bases his claims states only that this information "may" have been exposed to the malware because it was used at a Kimpton location during the at-risk window, not that it was actually captured and exfiltrated. (Open. Br., Ex. A at 1.) On these alleged facts, plaintiff's claim that his payment card information was "stolen" is speculative. (Open. Br. 4.)

B. Mitigation Efforts Alone Do Not Confer Standing To Sue.

Plaintiff also claims to have standing because he was "forced to spend time monitoring his credit." (Opp. 1, 6-7.) But plaintiff does not come to grips with the Supreme Court's holding in *Clapper v. Amnesty International USA*, 133 S. Ct. 1138, 1151 (2013), that parties "cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." The upshot of this holding is clear: incurring costs to mitigate the risk of potential future harm does not support standing unless the plaintiff can show the potential future harm is certainly impending, or at a minimum that there is a substantial risk that it will occur. "[W]hen the plaintiffs attempt to separate the standing issue regarding mitigation costs from that of the substantial risk of harm, they are ignoring the Supreme Court's directive in *Clapper*." *In re Community Health Systems, Inc., Cust. Sec. Data Breach Litig.*, 2017 WL 604334, at *7 (N.D. Ala. Feb. 15, 2017); *see also Fero v. Excellus Health Plan, Inc.*, --- F. Supp. 3d ---, 2017 WL 713660, at *10-11 (W.D.N.Y. Feb. 22, 2017) (same).

C. Plaintiff Does Not Have Standing Based on His Alleged Future Risk of Harm.

Plaintiff's last theory of standing is that "he remains at considerable risk for identity theft and fraud." (Opp. 1.) The rationale offered by plaintiff for this position is that he should not have "to wait until he actually suffers credit card fraud to have standing." (*Id.* at 6.)

The cases plaintiff cites for this point are distinguishable on their facts. *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), for example, did not involve payment cards, but

rather a stolen computer containing "unencrypted names, addresses and social security numbers of approximately 97,000 Starbucks employees." *Id.* at 1140. Moreover, unlike plaintiff here, one of the *Krottner* plaintiffs alleged that following the theft "someone had attempted to open a new account using his social security number." *Id.* at 1141. It was only "[o]n these facts," which are materially different than those present here, that the court in *Krottner* found the plaintiffs had standing to sue. *Id.* at 1143. In his opposition brief, plaintiff fails to address the significance of these distinguishing factors.

Similarly, the data breach in *In re Adobe Systems, Inc. Privacy Litigation*, 66 F. Supp. 3d 1197 (N.D. Cal. 2014), also implicated more information than what is at issue here, "including names, login IDs, passwords, credit and debit card numbers, expiration dates, and mailing and e-mail addresses." *Id.* at 1206. Moreover, one or more of the named plaintiffs in *Adobe* alleged that the information implicated in the data breach "has already surfaced on the Internet" and "black market websites." *See id.* at 1215 n.5, 1216. Again, plaintiff has failed to address these important distinctions.[2]

Plaintiff also relies on the Seventh Circuit's decisions in *Lewert v. P.F. Chang's Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016), and *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015). While those cases involved payment card breaches, they too are distinguishable because at least some of the named plaintiffs alleged fraudulent charges on their payment cards as a result of the breach. *See* 819 F.3d at 965; 794 F.3d at 691. Indeed, in *Remijas* there were already 9,200 instances of reported fraud following the malware attack, out of 350,000 individuals notified. 794 F.3d at 690.

The bottom line is that plaintiff's attempt to apply any of these decisions to the present case is inconsistent with the Supreme Court's holding in *Clapper*. Plaintiff argues that "[i]t cannot be seriously contested that the motivation behind the theft was to misuse the personal and

[2] Plaintiff also cites *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, --- F.3d ----, 2017 WL 242554, at *11 (3d Cir. Jan. 20, 2017), and *Galaria v. Nationwide Mut. Ins. Co.*, 2016 WL 4728027, at *3 (6th Cir. Sept. 12, 2016). But *Horizon* involved Congress's authority to confer statutory standing under the Fair Credit Reporting Act, which is not at issue here. And the unpublished *Galaria* decision is not binding even in the Sixth Circuit. *See Graiser v. Visionworks of Am., Inc.*, 819 F.3d 277, 283 (6th Cir. 2016). In any event, *Galaria*, like *Krottner*, is distinguishable in that it involved social security numbers, not payment card data.

payment card information of consumers[.]" (Opp. 4.) The same could probably be said of any payment card breach. But the fact that we have to speculate on this point at all is itself a strong indication why standing does not exist. *See Clapper*, 133 U.S. at 1150 (declining to "abandon our usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors"). And here, even if plaintiff's information was stolen, plaintiff has provided no basis for concluding that there is a substantial risk that *his* information, among all the other data affected by the malware attack, will ever be misused.

The Fourth Circuit's recent decision in *Beck* is instructive. There the court explained that the mere theft of a plaintiff's personal information does not meet *Clapper*'s requirement of a substantial risk of future harm, much less certainly impending harm, because even after acquiring the data, "the thieves must then select, from thousands of others, the personal information of the named plaintiff and attempt successfully to use that information to steal their identities." 2017 WL 477781, at *7, 8. The plaintiffs in *Beck* cited statistics purporting to show there was a 33% chance they would suffer identity fraud, but this too was not enough: "[I]t follows that over 66% of veterans affected will suffer no harm," the court explained, and thus "[t]his statistic falls far short of establishing a 'substantial risk' of harm." *Id.* at *9; *see also In re Science Applications Int'l Corp Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014) (rejecting argument that 9.5% increased chance for identity theft generally sufficient to provide standing; "The degree by which the risk of harm has increased is irrelevant – instead, the question is whether the harm is certainly impending.")

The Court should adopt *Beck*'s reasoning here. Countless millions of individuals are notified each year that their payment card information may potentially be at risk; it is a fact of present-day life. If all those individuals could bring suit now, without regard to whether they have yet suffered any identity fraud, or ever will, the federal courts would be overrun. This is why the strict standards that *Clapper* has placed on when the risk of future injury can support standing to sue should be respected in order to preserve the constitutional role of the federal courts. Plaintiff's amended complaint fails to meet *Clapper*'s requirements and therefore should be dismissed under Rule 12(b)(1).

II. PLAINTIFF ALSO HAS NOT STATED A CLAIM ON THE MERITS.

A. Plaintiff Has Not Alleged a Cognizable Injury for any of His Claims.

In his brief, plaintiff does not dispute that injury is an essential element of each of his claims. Instead, he proposes three different types of alleged harm to support his various causes of action: benefit of the bargain, diminution in value of personal information, and mitigation costs and efforts. (Opp. 10-14.) None of these are sufficient to support a claim on which relief can be granted as a matter of law.

1. Plaintiff Cannot Seek Damages Based on a Theory of Benefit of the Bargain or Overpayment.

Plaintiff seeks to support both his contract claim and his claim under the Unfair Competition Law (UCL) with "benefit of the bargain" damages, which he refers to in his amended complaint as an "overpayment." (*See* Opp. 1, 13-14; Am. Compl. ¶ 47(h).)

However labeled, the fundamental problem with plaintiff's claim for overpayment damages here is that he has not adequately alleged any facts to support it. All he has done is assert, in conclusory fashion, that he made "overpayments to Kimpton for products and services" because "a portion of the price paid for such products and services . . . was for the costs of reasonable and adequate safeguard and security measures," which Kimpton allegedly "did not implement." (Am. Compl. ¶ 47(h); *see also* Opp. 13 (claiming plaintiff "paid money to Kimpton for security he did not receive").) But nowhere in his amended complaint does he offer any factual allegations to explain how he bargained for data security or in any other way how the parties allocated a portion of the price for a hotel stay he indisputably received to data security. Courts in many cases have rejected similarly weak and conclusory assertions of overpayment as insufficient to provide standing, much less state a claim for damages. *See, e.g.*, *Fero*, 2017 WL 713660, at *11 (collecting cases on standing); *In re Barnes & Noble Pin Pad Litig.*, 2016 WL 5720370, at *5 (N.D. Ill. Oct. 3, 2016) (dismissing implied contract claim under California law for failure to allege actual damages; "*Remijas* specifically cast doubt on whether such harms would be sufficient even to establish standing, much less to establish out of pocket losses.").

Moreover, benefit of the bargain would not be an appropriate measure of damages for plaintiff's contract claim even if he had alleged facts to support such a theory. In data breach cases, as the court explained in *In re LinkedIn User Privacy Litig.*, 932 F. Supp. 2d 1089, 1094 (N.D. Cal. 2013), "[t]he economic loss Plaintiff alleges – not receiving the full benefit of his bargain – cannot be the 'resulting damages' of this alleged breach." Ignoring this authority, plaintiff instead relies on *Coughlin v. Blair*, 41 Cal.2d 587, 603 (1953), a unique case where the plaintiffs contracted for improvements on land they did not own. *Id.* at 600. But *Coughlin* itself recognized that in the typical case the purpose of contract damages is to place the plaintiff "in the same position he would have been in had the promisor performed the contract." *Id.* at 603.[3]

2. Diminution in Value.

Plaintiff also argues he has adequately alleged damages on his contract claim under a diminution in value theory, claiming "PII has a particular value." (Opp. 10.) But here too, plaintiff has not alleged any *facts* to demonstrate how the numbers or code on his payment card have any particular value to him. Although he alleges "there is a well-established national and international market" for his "PII and PCD" (Am. Compl. ¶ 47(g)), he does not allege he would or even could participate in this market. Notably, the sole case plaintiff cites on this point, *In re Facebook Privacy Litig.*, 572 F. App'x 494, 496 (9th Cir. 2014), has been interpreted to require allegations that the information at issue has lost value on some market in which plaintiff could participate. *See Svenson v. Google, Inc.*, 65 F. Supp. 3d 717, 724-25 (N.D. Cal. 2014) (analyzing *Facebook* and holding "as a matter of common sense a theory of diminished value would depend on the existence of a market for the information"). As the court held in *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010 (N.D. Cal. 2012), diminution in value is not a valid contract damages theory where plaintiffs had not "persuasively alleged that they reasonably expected that they would be compensated for the 'value' of their personal information." *Id.* at 1029; *see also*

[3] Plaintiff also cites *Svenson v. Google, Inc.*, 2015 WL 1503429, at *4 (N.D. Cal. Apr. 1, 2015). But *Svenson* relied on *Chavez v. Blue Sky Natural Beverage Co.*, 340 F. App'x 359, 361 (9th Cir. 2009), which was a consumer fraud case, not a breach of contract case. *Id.* at 360. In that situation, as in *Doe 1 v. AOL LLC*, 719 F. Supp. 2d 1102, 1111 (N.D. Cal. 2010), another case cited by plaintiff, difference in value damages might be an appropriate measure of damages. But that is not the correct measure of damages for breach of contract in a data theft case.

Gubala v. Time Warner Cable, Inc., 846 F.3d 909, 912-13 (7th Cir. 2017) (rejecting argument that alleged deprivation in value of personal information was sufficient to support standing, and stating: "This is gibberish.").

3. Time and Effort.

Finally, plaintiff argues he should be compensated for his alleged mitigation efforts, both in negligence and under a contract theory. (Opp. 11, 13.) Here plaintiff's opposition refers to alleged mitigation "costs" he "has already incurred[.]" (*Id.* at 11.) Plaintiff cites paragraph 13 of his amended complaint to support this assertion, but that paragraph carefully avoids any assertion that plaintiff paid for his "identity theft protection service." (Am. Compl. ¶ 13.)

Plaintiff also cites *In re Anthem, Inc. Data Breach Litigation*, 2016 WL 3029783, at *26 (N.D. Cal. May 27, 2016), to support his argument that time and effort alone is a recoverable harm. (Opp. 6, 7.) That decision is distinguishable inasmuch as it involved social security numbers and medical and employment information. *Id.* at *2. The court also relied on decisions from the standing context to allow a claim for damages under Rule 12(b)(6). *Id.* at *25-26 (*citing Lewert*, 819 F.3d at 967; *Remijas*, 794 F.3d at 694; *Smith v. Triad of Al., LLC*, 2015 WL 5793318, at *8-9 (M.D. Ala. Sept. 29, 2015); *In re Adobe Sys.*, 66 F. Supp. 3d at 1214). As the Ninth Circuit held in *Krottner*, however, simply because a plaintiff has standing does not mean he has stated a viable claim for damages. *Krottner v. Starbucks Corp.*, 406 F. App'x 129, 131 (9th Cir. 2010); *Pisciotta v. Old Nat. Bancorp*, 499 F.3d 629, 639 (7th Cir. 2007) (same). Notably, in both *Remijas* and *Lewert*, the court refrained from making any determinations on the merits of the plaintiffs' claims. *Remijas*, 794 F.3d at 697 ("the question whether this complaint states a claim on which relief can be granted is not properly before us"); *Lewert*, 819 F.3d at 970 (same).

In short, time and effort are not cognizable damages, but instead merely are part of "the ordinary frustrations and inconveniences that everyone confronts in daily life." *In re Hannaford Bros. Co. Cust. Data Breach Sec. Litig.*, 4 A.3d 492, 496-97 (Me. 2010); *see also Holmes v. Countrywide Fin. Corp.*, 2012 WL 2873892, at *10-11 (W.D. Ky. Jul. 12, 2012) ("Courts considering risk-of-identity-theft cases uniformly reject attempts to recover for the time the plaintiffs spent self-monitoring financial accounts and credit history."). As the Seventh Circuit

explained in *Pisciotta*: "Without more than allegations of increased risk of future identity theft, the plaintiffs have not suffered a harm that the law is prepared to remedy." 499 F.3d at 639-40.[4]

B. Plaintiff's Claims Fail for Additional Reasons as Well.

In addition to the deficiencies identified above, plaintiff' negligence claim is barred by the economic loss rule, his implied contract claim fails for lack of consideration and mutual assent, and he has not adequately pleaded his UCL fraud claim under Rule 9(b).

1. The Economic Loss Rule Bars Plaintiff's Negligence Claim.

Plaintiff relies on *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 988 (2004), to avoid the economic loss rule, arguing that under *Robinson* the rule does not apply because of Kimpton's "independent duty to securely maintain PII." (Opp. 12-13.) But *Robinson* made clear that the independent duty exception to the economic loss rule is "narrow in scope" and limited to "fraud and intentional misrepresentation claims." 34 Cal. 4th at 988, 993. Plaintiff suggests that a public policy favoring the protection of personal information justifies extending the independent duty exception to negligence claims in data breach cases (*see* Opp. 13), but cites no case law to support this position. In fact, courts in data breach cases have repeatedly rejected the argument that the independent duty exception saves negligence claims from the economic loss rule under California law. *See, e.g., Dugas*, 2016 WL 6523428, at *12; *In re Sony Gaming*, 996 F. Supp. 2d at 968; *In re Target Corp. Data Sec. Breach Litig.*, 66 F. Supp. 3d 1154, 1172 (D. Minn. 2014).

2. Plaintiff Has Not Alleged an Implied Contract for Data Security.

As Kimpton explained in its opening brief, plaintiff's implied contract theory fails for lack of consideration under California law because Kimpton was under a pre-existing duty to protect his confidential information. (Open. Br. 10.) In his opposition brief, plaintiff argues the pre-existing duty rule does not apply because Kimpton made additional statements in its website privacy policy that "do[] not simply mirror California law as to property security measures."

[4] Plaintiff attempts to undercut this holding in *Pisciotta* by pointing out that the Indiana legislature subsequently amended its statute to require companies to maintain reasonable procedures to safeguard information. (Opp. 12.) This is irrelevant. Indeed, the amended provision remains enforceable only by the Attorney General, *see* Ind. Code § 24-4.9-3-3.5(d), (e), and the statute still "imposes no duty to compensate affected individuals for inconvenience or harm to credit that may follow." *See* 499 F.3d at 637.

(Opp. 8.) In particular, plaintiff argues Kimpton impliedly promised not to "*disclose* PII except in compliance with the privacy policy." (*Id.* (emphasis added).)

The problem with this argument is that Kimpton did *not* disclose plaintiff's information in connection with the malware attack; if anything, this information was stolen from Kimpton. *See Fero*, 2017 WL 713660, at *36 ("in order to 'disclose' something, the information holder must commit some affirmative, voluntary act") (quotation omitted). Whatever promises or representations regarding disclosure that plaintiff purports to find in Kimpton's privacy policy are irrelevant for the simple reason that Kimpton never disclosed plaintiff's information. Thus, plaintiff's attempt to establish consideration for his implied contract claim on this basis fails.

The contract claim also fails for lack of mutual assent. Plaintiff argues he has satisfied this element because Kimpton, in its privacy policy, "implie[d] that Plaintiff's data will be secure." (Opp. 9.) But plaintiff has based his complaint on statements in the privacy policy that go to how Kimpton uses and discloses the information in its possession, rather than any statement regarding data security. (Am. Compl. ¶ 15.) Plaintiff is left with nothing more than his own "unilateral and subjective" expectations on this point, which is not enough to state a claim. *Lovell v. P.F. Chang's China Bistro, Inc.*, 2015 WL 4940371, at *3 (W.D. Wash. Mar. 27, 2015).

3. Plaintiff's UCL Fraud Claim Is Also Deficient.

Plaintiff does not respond to Kimpton's argument that he has failed to plead his omission claim with particularity as required by Rule 9(b). And he fails to address Kimpton's argument that no duty to disclose should be imposed because public safety is not at issue here. (*Id.* at 14.) He has therefore abandoned his omission claim. *See Zaklit v. Glob. Linguist Sols., LLC*, 2014 WL 12521725, at *13 (C.D. Cal. Mar. 24, 2014) (collecting cases holding party abandons claim by failing to respond to arguments raised in opening brief).

Plaintiff argues he has adequately pled an affirmative misrepresentation claim because "Kimpton's privacy policy represents to consumers the specific set of authorized disclosures of Plaintiff's PII to third parties that may occur." (Opp. 14.) But here again, plaintiff is overlooking the crucial distinction, recognized by many courts, between a purposeful disclosure and a theft. *See Fero*, 2017 WL 713660, at *37 ("Plaintiffs have not plausibly alleged a claim under either

statute where they have only alleged that their personal information was stolen from Defendants, not that Defendants disclosed the data to the cyberattackers."); *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 589760, at *39-40 (N.D. Cal. Feb. 14, 2016) (same); *compare Dolmage v. Combined Ins. Co. of Am.*, 2015 WL 292947, at *4 (N.D. Ill. Jan. 21, 2015) (holding plaintiff in alleged data breach case "does not, and cannot, plausibly allege that Defendant furnished or actively transmitted her personal information to the identity thieves"). Indeed, plaintiff's own cited case, *In re Sony Gaming*, illustrates the distinction because in that case the plaintiffs alleged Sony represented that it used industry-standard encryption to prevent unauthorized access to sensitive financial information. 996 F. Supp. 2d at 990. Plaintiff does not allege or rely on any similar statement in Kimpton's privacy policy.

Finally, plaintiff argues the Court must presume his alleged reliance on Kimpton's claimed misrepresentations because they generally appeared on Kimpton's website. (Opp. 15.) With the enactment of Proposition 64, however, California law now "imposes an actual reliance requirement on plaintiffs prosecuting a private enforcement action under the UCL's fraud prong." *In re Tobacco II Cases*, 46 Cal. 4th 298, 326 (2009). In *Tobacco II*, the court held that reliance may only be presumed in cases like that one, which involved an "extensive" and "long-term" advertising campaign. *Id.* at 327. As the Ninth Circuit has subsequently held, "California courts have recognized that *Tobacco II* does not allow a consumer who was *never exposed* to an alleged false or misleading advertising campaign to recover damages under California's UCL." *Mazza v. Am. Honda Motor Co., Inc.*, 666 F.3d 581, 596 (9th Cir. 2012) (emphasis added). That is precisely the situation plaintiff alleges here, and his UCL fraud claim should be dismissed.

CONCLUSION

The Court should grant Kimpton's motion to dismiss.

Dated: March 7, 2017

BAKER & HOSTETLER LLP

By: */s/ Daniel R. Warren*
DANIEL R. WARREN

Attorney for Defendant
KIMPTON HOTEL & RESTAURANT GROUP, LLC

BAKER & HOSTETLER LLP
ATTORNEYS AT LAW
LOS ANGELES