ORIGINAL

Rosemary M. Rivas (State Bar No. 209147)
rrivas@finkelsteinthompson.com
Mark Punzalan (State Bar No. 247599)
mpunzalan@finkelsteinthompson.com
Danielle A. Stoumbos (State Bar No. 264784)
dstoumbos@finkelsteinthompson.com
FINKELSTEIN THOMPSON LLP
100 Bush Street, Suite 1450
San Francisco, California 94104
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

Counsel for Plaintiff Dao Phong

Paid
$350

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

DAO PHONG, an individual, on behalf of herself and all others similarly situated,

Plaintiff,

vs.

CARRIER IQ, INC.; and HTC AMERICA, INC.,

Defendants.

Case No. CV 11-06333 HRL

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiff Dao Phong ("Plaintiff"), individually and on behalf of all others similarly situated, alleges as follows based on her counsel's investigation and her personal experience:

INTRODUCTION

1. Plaintiff brings this action for actual damages, equitable relief (including restitution, injunctive relief, and disgorgement of profits), civil penalties, and all other available relief on behalf of herself and all similarly-situated individuals and entities in the United States who, within four years of the filing of this litigation, bought a phone manufactured by Defendant HTC America, Inc. ("HTC") embedded with technology created and employed by Defendant Carrier IQ, Inc. ("Carrier IQ") (the "Class").

FAXED

2. All of the claims asserted herein arise out of Carrier IQ and HTC's misconduct in connection with the Carrier IQ "rootkit" software application that is installed in more than 140 million mobile phones. Based on information and belief, Plaintiff and Class members were not informed of the presence of Carrier IQ software on their phones at the time of purchase.

3. According to a recent analysis conducted by computer security researcher Trevor Eckhart, Carrier IQ software tracks and collects information related to every keystroke performed by the mobile phone user without disclosing this invasive technology to users. Carrier IQ software tracks and collects a wealth of private information these users perform on their phones such as when users turn their phones on and off, what phone numbers users dial, the contents of users' text messages, the websites users visit, the search terms users input into browsers, and the locations of users' phones. Based on information and belief, Carrier IQ then intentionally divulges information from mobile phone users to its clients, which include Handset Manufacturers such as HTC.

4. As alleged herein, Carrier IQ's conduct violates the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.* (the "Wiretap Act"); the Stored Communications Act of 1986 ("SCA"), 18 U.S.C. §§ 2701, *et seq.*; California's Computer Crime Law ("CCCL"), Cal. Penal Code § 502, *et seq.*; and California's Unfair Competition Law, Bus. & Prof. Code § 17200, *et seq.*

THE PARTIES

5. Plaintiff Dao Phong is a citizen and resident of San Francisco, California. Plaintiff purchased an HTC Evo mobile phone manufactured by Defendant HTC and activated and maintained cellular service for this phone with Sprint. As a result of the misconduct alleged herein, Plaintiff has suffered injury in fact and has lost money or property.

6. Defendant Carrier IQ is a Delaware corporation with its principal place of business located at 1200 Villa Street, Suite 200, Mountain View, California 94041. Based on information and belief, Carrier manufactures and supports a "rootkit" software application that is installed in mobile phones by manufacturers.

7. Defendant HTC America, Inc. is a Washington corporation with its principal place of business located at 811 1st Ave., Suite 530, Seattle Washington 98104.

//

JURISDICTION

8. Pursuant to 28 U.S.C. 1331, this Court has original jurisdiction over this lawsuit arising under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2511, *et seq*. This Court also has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a class action in which: (1) there are 100 or more members in the Plaintiff's proposed class; (2) at least some members of the proposed class have a different citizenship from one or more Defendants; and (3) the claims of the proposed class members exceed $5,000,000 in the aggregate.

9. This Court also has personal jurisdiction because Defendants have purposefully availed themselves of the privilege of conducting business activities by advertising, contracting, and conducting services within the State of California and have generally maintained systematic and continuous business contacts with the State of California. Defendant Carrier IQ is also headquartered in California.

VENUE AND INTRADISTRICT ASSIGNMENT

10. Venue is proper in the Northern District of California and in the San Jose Division, pursuant to 28 U.S.C. section 1391 subsections (b) and (c), and Civil L.R. 3-2 subsections (c) and (e). A substantial part of the events giving rise to the claims at issue in this litigation occurred in this District and Division because Defendants advertised, contracted, and conducted its services in this District and Division. Additionally, Defendant Carrier IQ is present in this Judicial District and Division and transacts business in this Judicial District and Division.

FACTUAL ALLEGATIONS

11. Carrier IQ manufactures and supports a "rootkit" software application that is installed in mobile phones by manufacturers such as HTC. According to Carrier IQ, its software application is installed on over 140 million handsets and mobile phones.

12. On its website, Carrier IQ markets itself as "the only company embedding diagnostic software in millions of subscribers' phones" and purports to track "Actionable Intelligence" on mobile phones. The Company markets itself to wireless carriers and handset manufacturers as the only company that "collects, correlates and aggregates data" in mobile phones "for near real-time system monitoring and business intelligence." Carrier IQ also states that its software performs these functions "with no visible impact to [] customers."

13. A recent analysis performed by computer security researcher Trevor Eckhart reveals that Carrier IQ's software performs functions that are extremely intrusive to users' privacy. In a video posted on YouTube, Mr. Eckhart demonstrates that Carrier IQ software can log every keystroke that the user performs on her mobile phone.[1] The Eckhart video reveals that for the 140 million phones embedded with the Carrier IQ software, Carriers IQ can track and collect a wealth of information by tracking these keystrokes. For instance, Carrier IQ can collect information when users turn their phones on and off, the phone numbers they dial, the contents of their text messages, the websites they visit, the search terms they input into browsers, and their phones' locations. Carrier IQ can also collect these data even when such data are supposed to be transmitted securely, *e.g.*, by HyperText Transfer Protocol over Secure Socket Layer ("https").[2] Moreover, Carrier IQ can collect data for the location of the users' phone even when the user has expressly denied location access to the phone's location.

14. Based on information and belief, neither Carrier IQ or HTC disclose to mobile phone users that Carrier IQ software is embedded in their phone and that the software tracks and collects users' actions. Based on information and belief, Carrier IQ software does not make itself readily apparent to a user and does not show up in a phone's list of active processes. Even if a technologically-savvy user is able to find out that Carrier IQ is running, users are not given an option to shut down the software.

15. Based on information and belief, once Carrier IQ collects these data from mobile phone users, it provides this information to its clients, which include Handset Manufacturers such as Defendant HTC. As the company states on its website, Carrier IQ "give[s] Wireless Carriers and Handset Manufacturers unprecedented insight into their customers' mobile experience." Carrier IQ further states that it provides "real-time data direct from [...] customers' handsets." Wireless carriers AT&T Inc., T-Mobile, and Sprint (Plaintiff's wireless carrier) have admitted that Carrier IQ is present on their phones.

16. After news outlets reported on Eckhart's analysis of Carrier IQ, Carrier IQ issued a statement denying that its software tracked usage or recorded keystrokes. This statement, however, is

---

[1] The full video is available at http://www.youtube.com/user/TrevorEckhart#p/u/0/T17XQI_AYNo (last visited Dec. 1, 2011).

[2] http://en.wikipedia.org/wiki/HTTP_Secure

apparently not only contradicted by the Company's own website representations but by the company's own patent application for its software, in which the company describes its technology as a "method for collecting data at a server coupled to a communications network, comprising: transmitting to a device a data collection profile… wherein the set of data relates to an end user's interaction with the device… [and] wherein the interaction with the device comprises the end user's pressing of keys on the device."

17. According to recent news reports, after Mr. Eckhart publicly expressed concerns over Carrier IQ's capabilities, Carrier IQ sent a cease-and-desist letter threatening a lawsuit. Carrier IQ withdrew this threat and publicly apologized after a non-profit group intervened on Mr. Eckhart's behalf. Since news reports were released regarding Carrier IQ's tracking of users' mobile phones, Senator Al Franken (D-MN) also opened a probe into Carrier IQ. Senator Franken described the allegations surrounding Carrier IQ as "deeply troubling" and said that Congress should act "quickly" to protect consumers' privacy.

STATUTES OF LIMITATION

18. **Discovery Rule.** The causes of action alleged herein accrued upon discovery of Carrier IQ's wrongful conduct. Because telephone users could not readily determine their phones contained Carrier IQ software and Carrier took steps to actively conceal them, Plaintiff and members of the Class did not discover and could not have discovered Carrier IQ's wrongful conduct through reasonable and diligent investigation. Moreover, reasonable and diligent investigation into Carrier IQ's wrongful conduct did not and could not reveal a factual basis for a cause of action based on Carrier IQ's nondisclosure or concealment of its actions.

CLASS ACTION ALLEGATIONS

19. Plaintiff brings this lawsuit as a class action on behalf of herself and all others similarly situated as members of a proposed plaintiff Class pursuant to Federal Rule of Civil Procedure 23. This action satisfies the ascertainability, numerosity, commonality, typicality, adequacy, predominance and superiority requirements of those provisions.

20. The Class is initially defined as:

> *All persons and entities residing in the United States who purchased an HTC device embedded with Carrier IQ software.*

21. Excluded from the Class are (1) HTC and Carrier IQ, any entity in which HTC or Carrier IQ have a controlling interest, and their legal representatives, officers, directors, employees, assigns and successors, and (2) the judge to whom this case is assigned and any member of the judge's immediate family.

Numerosity and Ascertainability

22. On information and belief, the Class is comprised of millions of people, making joinder impractical. As of December 2, 2011, Carrier IQ's website purports that Carrier IQ software is embedded in more than 141 million handsets. Many of these handsets are persons who purchased an HTC device.

23. The Class is composed of an easily ascertainable, self-identifying set of individuals and entities who bought an HTC phone embedded with Carrier IQ technology in the four years leading up to this litigation. Discovery will be used to populate the list of members of the Class.

Community of Interest

24. There is a well-defined community of interest among the Class members, and the disposition of their claims in a single action will provide substantial benefits to all parties and to the Court.

Typicality

25. The claims of the Representative Plaintiff are typical of the claims of the Class, in that the Representative Plaintiff, like all members of the Class, bought an HTC phone embedded with Carrier IQ software. The factual bases of the misconduct alleged herein are common to all Class members and represent a common thread of fraudulent misconduct resulting in injury to all members of the Class.

Predominance of Common Issues

26. There are numerous questions of law and fact common to all Class members, and those questions predominate over any questions that may affect only individual Class members.

27. The predominant questions include the following:

a. Whether Defendants conducted the common business practice of collecting, tracking, and sharing with third parties the private mobile phone actions performed by users;

b. Whether Defendants failed to disclose to Plaintiff and the Class that its software collected, tracked, and shared with third parties their private mobile phone actions;

c. Whether Defendants knew and/or were reckless in not knowing of the unlawful nature of their conduct;

d. Whether Defendants had a duty to Plaintiff and the Class to disclose their wrongful conduct;

e. Whether Defendants' conduct violated the The Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*, the Stored Communications Act of 1986 ("SCA"), 18 U.S.C. § 2711(1), and California's Computer Crime Law, Cal. Penal Code § 502; and

f. Whether Defendants' active concealment of and/or failure to disclose the true nature of its conduct was likely to mislead or deceive, and was therefore fraudulent, within the meaning of Cal. Bus. & Prof. Code § 17200, *et seq.*

Adequacy

28. Plaintiff will fairly and adequately represent and protect the interests of the Class. Plaintiff has retained counsel with substantial experience in prosecuting consumer class actions, including actions involving privacy issues and the claims alleged herein.

29. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the Class, and have the financial resources to do so. Neither Plaintiff nor her Counsel have interests adverse to those of the Class.

Superiority

30. Absent class treatment, Plaintiff and members of the Class will continue to suffer harm and damages as a result of Defendants' unlawful and wrongful conduct.

31. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Without a class action, individual Class members would face burdensome litigation expenses, deterring them from bringing suit or adequately protecting their rights. Because of the modest economic value of the individual Class members' claims, few if any could seek their rightful legal recourse in an individual action. Absent a class action, Class members would

continue to incur harm without remedy, while Defendants would continue to reap the benefits of its misconduct.

32. The consideration of common questions of fact and law will conserve judicial resources and promote a fair and consistent resolution of these claims.

FIRST CAUSE OF ACTION
(Violation of the Wiretap Act)

33. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

34. The Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.* (the "Wiretap Act") broadly defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in party by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce..." 18 U.S.C. § 2510(12).

35. Pursuant to the Wiretap Act, Defendants operate an "electronic communications service" as defined in 18 U.S.C. § 2510(15).

36. The Wiretap Act broadly defines the contents of a communication. Pursuant to the Wiretap Act, "contents" of a communication, when used with respect to any wire, oral, or electronic communications, include any information concerning the substance, purport, or meaning of that communication. 18 U.S.C. § 2510(8). "Contents," when used with respect to any wire or oral communication, includes any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication. The definition thus includes all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded. The privacy of the communication to be protected is intended to be comprehensive.

37. The Wiretap Act prevents an electronic communications service operator from intentionally divulging the contents of any communication while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication. 18 U.S.C. § 2511(3)(a). Plaintiff and Class members are "person[s] whose ... electronic communication[s] [are] disclosed... or intentionally used in violation of this chapter" within the meaning of 18 U.S.C. § 2520(a). When users perform such functions on their phone as turning their phones on and off, dialing phone

numbers, sending text messages, visiting websites, users are unknowingly sending electronic communications to Defendants. Users do not expect and do not consent to any disclosure of the activities to their phone to Defendants or to any third parties to whom Defendants makes this information available.

38. Based on information and belief, Defendants intentionally divulge the electronic communications of mobile phone users to third parties. By divulging these communications and other user information to third parties without user consent, Defendants intentionally violated 18 U.S.C. § 2511(3)(a).

39. Each incident in which Defendants divulged the electronic communications of mobile phone users is a separate and distinct violation of the ECPA. Plaintiff and members of the Class therefore seek remedies as provided for by 18 U.S.C. § 2520, including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and attorneys' fees and other litigation costs reasonably incurred.

40. Plaintiff and the Class, pursuant to 18 U.S.C. § 2520(2), are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of the greater of $10,000 or $100 a day for each day of violation, actual and punitive damages, reasonable attorneys' fees, and Defendants' profits obtained from the violations described herein.

SECOND CAUSE OF ACTION

(Violations of the Stored Communications Act)

41. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

42. The Stored Communications Act of 1986 ("SCA") incorporates the Wiretap Act's definition of an "electronic communication service." 18 U.S.C. § 2711(1). As set forth above, Defendants are electronic communications service providers within the meaning of the ECPA and is therefore also subject to the restrictions contained in the SCA governing electronic communications service providers. The SCA also incorporates the Wiretap Act's broad definition of "electronic communication" and "electronic storage." 18 U.S.C. § 2711(1). Pursuant to the Wiretap Act and the SCA, "electronic storage" means any "temporary storage of a wire or electronic communication

incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). This type of electronic storage includes communications in intermediate electronic storage that have not yet been delivered to their intended recipient.

43. The SCA prohibits any electronic communications service provider from divulging to any person or entity the contents of a communication while in electronic storage by that service. 18 U.S.C. § 2702(a)(1). Based on information and belief, Defendants provide this information to third parties. When users perform functions on their phones such as making a phone call, sending a text message, or browsing the internet, users do not expect, intend and consent for Carrier IQ to collect and track this information or pass along the communications to a third party as a handset manufacturer. Based on information and belief, Defendants provide users' information regarding electronic communications to third parties in violation of 18 U.S.C. § 2702(a)(1). By disclosing these communications, Defendants violated 18 U.S.C. § 2702(a)(1).

44. The SCA definition of "electronic storage" also includes "storage of [a wire or electronic] communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(B). The information that Defendants collect from users via electronic communications are electronically stored by Defendants for backup purposes.

45. The SCA, at 18 U.S.C. § 2702(a)(2), provides that "a person or entity providing a remote communication service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carrier or maintained on that service (A) on behalf of, and received by means of electronic transmission...a subscriber or customer of such service; (B) solely for the purpose of providing storage...to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."

46. Plaintiff and Class members are "person[s] aggrieved by [a] violation of [the SCA] in which the conduct constituting the violation is engaged in with a knowing or intentional state or mind..." within the meaning of 18 U.S.C. § 2707(a).

//

//

47. Each incident in which Defendants divulged users' stored communications to a third party is a separate and distinct violation of the SCA, subject to the remedies provided under the SCA, and specifically pursuant to 18 U .S.C. § 2707(a).

48. Plaintiff and the Class therefore seek remedies as provided for by 18 U.S.C. § 2707(b) and (c), including such preliminary and other equitable or declaratory relief as may be appropriate, damages consistent with subsection (c) of that section to be proven at trial, punitive damages to be proven at trial, and attorneys' fees and other litigation costs reasonably incurred.

49. Plaintiff and the Class, pursuant to 18 U.S.C. § 2707(c), are entitled to preliminary, equitable, and declaratory relief, in addition to statutory damages of no less than $1,000 per violation, actual and punitive damages, reasonable attorneys' fees, and Defendants' profits obtained from the violations described herein.

THIRD CAUSE OF ACTION

Violation of California's Computer Crime Law ("CCCL"), Cal. Penal Code § 502

50. Plaintiff incorporates the foregoing allegations as if fully set forth herein.

51. Defendants knowingly accessed and without permission used any data, computer, computer system, or computer network in order to execute a scheme or artifice to deceive and/or to wrongfully control or obtain money, property, or data in violation of Cal. Penal Code § 502(c)(1).

52. Defendants did so by accessing and sharing with wireless carriers and handset manufacturers the mobile phone actions of Plaintiff and Class members in order to deceive and/or to wrongfully profit by collecting, tracking and disclosing users' information.

53. Defendants knowingly accessed and without permission took, copied, or made use of Plaintiff and Class members' information regarding actions performed on their mobile phones in violation of § 502(c)(2).

54. Defendants knowingly and without permission used or caused to be used computer services by impermissibly accessing, collecting, and transmitting Plaintiffs' and Class members' personal information in violation of § 502(c)(3).

55. Defendants knowingly and without permission provided or assisted in providing a means of accessing a computer, computer system, or computer network by creating a system that allowed third parties to impermissibly access, collect, and transmit Plaintiffs' and Class members' private mobile phone actions in violation of § 502(c)(6).

56. Defendants knowingly and without permission accessed or caused to be accessed Plaintiff and Class members' computers and/or computer networks by impermissibly divulging Plaintiffs' and Class members' personal information to advertisers in violation of § 502(c)(7). Defendants knowingly and without permission introduced a computer contaminant, as defined in § 502(b)(10), by introducing computer instructions designed to record or transmit to third parties Plaintiff and the Class' private actions performed on their phones on Defendants' computer networks without the intent or permission of Plaintiff or the Class in violation of § 502(c)(8). These instructions usurped the normal operations of the relevant computers, which by normal operation would not transmit the private mobile phone information of Plaintiff and/or the Class members.

57. As a direct and proximate result of Defendants' violation of § 502, Defendants caused loss to Plaintiff and the Class members in an amount to be proven at trial. Plaintiff and the Class are entitled to the recovery of attorneys' fees pursuant to § 502(e).

58. Plaintiff and Class members have also suffered irreparable injury as a result of Defendants' unlawful conduct, including the collection and sharing of their personal mobile phone information. Additionally, because the stolen information cannot be returned, the harm from this breach is ongoing and compounding. Accordingly, Plaintiff and the Class have no adequate remedy at law, entitling them to injunctive relief.

FOURTH CAUSE OF ACTION

Violation of California's Unfair Competition Law
Cal. Bus. & Prof. Code § 17200, *et seq.*

59. Plaintiff incorporates the foregoing allegations as if fully set forth herein. California Business & Professions Code § 17200, *et seq.* ("UCL"), prohibits acts of "unfair competition." The UCL defines unfair competition as any unlawful, unfair, or fraudulent business act or practice. Thus,

under the UCL, there are three categories of unfair competition: conduct that is unlawful, conduct that is unfair, and conduct that is fraudulent.

60. Defendants violated the UCL by engaging in conduct that violated each of the three prongs of the statute.

61. Defendants' practice of, among other things, collecting and tracking keystrokes by users and disclosing them to third parties is unlawful because it violates, among other things, the Wiretap Act, the SCA, and CCCL, as alleged above.

62. Defendants engaged in unfair business practices by, among other things:

g. Engaging in conduct that causes a substantial injury to consumers, specifically by disclosing their private mobile information to third parties. Defendants' practices are not outweighed by any countervailing benefits to consumers or to competition. Consumers could not have reasonably avoided this injury.

h. Engaging in conduct that is immoral, unethical, oppressive, unscrupulous, or substantially injurious to Plaintiff and other members of the Class; and

i. Engaging in conduct that undermines or violates the stated policies underlying the SCA, Wiretap Act, and CCCL.

63. Defendants engaged in fraudulent business practices by concealing and/or failing to disclose the true nature and characteristics of its collection, tracking, and disclosure of private mobile phone information. Defendants had a duty to disclose such information by virtue of their exclusive knowledge, among other things.

64. As a direct and proximate result of Defendants' violation of Cal. Bus. & Prof. Code § 17200, *et seq.*, Plaintiff suffered injury in fact and lost money or property, in that she paid money to purchase her phone. Plaintiff and the Class members are entitled to monetary relief, including restitution of all amounts that Defendants billed and collected, as well as attorneys fees under Cal. Code of Civ. P. § 1021.5. Further, as a result of Defendants' violation of the UCL, Defendants have been unjustly enriched and should be required to make restitution to Plaintiff and the Class or to disgorge its ill-gotten profits pursuant to Cal. Bus. & Prof. Code § 17203.

65. Plaintiff and the Class members are entitled to equitable relief, including declaratory relief and a permanent injunction enjoining Defendants from continuing their unlawful, unfair, and fraudulent billing practices.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for relief and judgment against Defendant as follows:

A. Certifying the Class pursuant to Rule 23 of the Federal Rules of Civil Procedure, certifying Plaintiff as representative of the Class, and designating her counsel as counsel for the Class;

B. Awarding Plaintiff and the Class compensatory damages, in an amount exceeding $5,000,000, to be determined by proof;

C. Awarding Plaintiff and the Class statutory damages;

D. Requiring Defendants to make restitution and/or disgorgement;

E. Imposition of a constructive trust for the benefit of Plaintiff and the Class on all monies wrongfully taken or received by Defendants;

F. Equitable and declaratory relief, and an order enjoining Defendants from continuing to engage in the wrongful acts and practices alleged herein;

G. Awarding Plaintiff and the Class the costs of prosecuting this action, including expert witness fees;

H. Awarding Plaintiff and the Class reasonable attorney's fees;

I. Awarding pre-judgment and post-judgment interest; and

J. Granting other relief as this Court may deem just and proper under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury of all claims so triable.

DATED: December 14, 2011

FINKELSTEIN THOMPSON LLP

By: _____
Mark Punzalan

Rosemary M. Rivas
Danielle A. Stoumbos
100 Bush Street, Suite 1450
San Francisco, California 94104
Telephone: (415) 398-8700
Facsimile: (415) 398-8704

Counsel for Plaintiff Dao Phong