UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

AT&T MOBILITY LLC, Plaintiff, v. MARC SAPATIN, SAPATIN NGUYEN ENTERPRISES, INC., SAPATIN ENTERPRISES, INC., NGUYEN LAM, KYRA EVANS, PRASHANT VIRA, SWIFT UNLOCKS, INC. and JOHN DOES 1-50, United States individuals and entities, Defendants.	No. COMPLAINT FOR DAMAGES AND INJUNCTIVE RELIEF **JURY TRIAL DEMANDED**

Plaintiff AT&T Mobility LLC ("AT&T") hereby files this Complaint for Damages and Injunctive Relief against Defendants Marc Sapatin, Sapatin Nguyen Enterprises, Inc., Sapatin Enterprises, Inc., Nguyen Lam, Kyra Evans, Prashant Vira, Swift Unlocks, Inc. and John Does 1-50 and states:

NATURE OF ACTION

1. This is an action for damages arising out of Defendants' participation in a conspiracy to fraudulently abuse AT&T's computer systems in order to illegally "unlock" wireless telephones used on AT&T's network.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

2. As set forth in greater detail below, Defendants engaged in, and knowingly facilitated and encouraged others to engage in, a scheme using an unauthorized computer program to attack AT&T's protected computer systems and illegally "unlock" wireless phones for use on other networks (the "Unlock Scheme").

3. "Unlocking" a phone disables certain software pre-installed by the phone manufacturers, which is designed to limit the activation of the phones exclusively to AT&T's network. Once a phone is unlocked, it can be used on multiple carrier systems rather than exclusively with AT&T.

4. The software is vital to AT&T's business because it allows AT&T to subsidize the cost of the phone to consumers while protecting AT&T's investment in the phones through term contracts. The software also protects AT&T's goodwill with respect to phones that carry AT&T's brand, because some of the phones' functionality may not work as effectively on non-AT&T networks.

5. Defendants perpetuated the Unlock Scheme by creating, distributing, and placing on AT&T's computer systems a "malware" program designed to fraudulently, and without authorization, transmit unlock requests that unlocked hundreds of thousands of phones from exclusive use on AT&T's network.

6. Through this conduct, the Unlock Scheme caused substantial damage to AT&T's protected computer systems and effectively stole AT&T's subsidy investment in its phones.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

PARTIES

7. Plaintiff AT&T Mobility LLC is a limited liability company organized and existing under the laws of the state of Delaware. AT&T's principal place of business is 1025 Lenox Park Boulevard NE, Atlanta, Georgia 30319.

8. Defendant Marc Sapatin is an individual resident of the state of Washington. Sapatin may be served with a summons and a copy of this complaint at 6713 74th Drive NE, Marysville, WA 98270-6506.

9. Defendant Nguyen Lam is an individual resident of the state of Washington. Lam may be served with a summons and a copy of this complaint at 9905 32nd Drive SE, Everett, WA 98208-3100.

10. Defendant Kyra Evans is an individual resident of the state of Washington. Evans may be served with a summons and a copy of this complaint at 1002 12th Street, No. 208, Auburn, WA 98002-6271.

11. Defendant Sapatin Nguyen Enterprises, Inc. ("SNE") is a corporation organized and existing under the laws of the state of Washington. Filings made with the Washington Secretary of State do not identify SNE's principal place of business, but state that its President, Treasurer, and Chairman, Marc Sapatin, is located at 15907 Ash Way, Apt. C202, Lynnwood, Washington 98087 and that its Vice-President and Secretary, Mike Nguyen, is located at 12303 Harbour Pointe Boulevard, Apt. C208, Mukilteo, Washington 98275. SNE may be served through its registered agent for service of process, Marc Sapatin, at 20815 67th Avenue West, Suite 202/203, Lynwood, Washington 98036-7359, or through any office, managing or general agent, or other agent authorized by appointment or law to receive service of process at the office address denoted above.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

12. Defendant Sapatin Enterprises Inc. ("SE") is a corporation organized and existing under the laws of the state of Washington. Filings made with the Washington Secretary of State do not identify SNE's principal place of business, but state that SE's address is P.O. Box 2424, Lynnwood, Washington 98036. SE may be served through its registered agent for service of process, Marc Sapatin, at 19131 56th Avenue West, Lynnwood, Washington 98036, or through any office, managing or general agent, or other agent authorized by appointment or law to receive service of process at the office address denoted above.

13. Defendant Prashant Vira is an individual doing business as Swift Unlocks and residing in the state of California. Vira may be served with a summons and a copy of this complaint at 8504 East Woodcove Dr., #126, Anaheim, California 92808.

14. Defendant Swift Unlocks, Inc. is a corporation organized and existing under the laws of the state of California. Its principal place of business is 751 S. Weir Canyon Road, Suite 157-345, Anaheim, California 92808. Swift Unlocks may be served through its registered agent for service of process, Michael S. Weigold, at 635 N. Eckhoff Street, Suite B, Orange, California 92868, or through any office, managing or general agent, or other agent authorized by appointment or law to receive service of process at the office address denoted above.

15. Upon information and belief, John Doe Defendants 1-50 jointly participated in the development of software used in the illegal and fraudulent scheme at issue in this complaint, the provision of that software to current and former AT&T employees, payment to current and former AT&T employees for their unauthorized installation of the software on AT&T's protected computer systems, and the resale of phones that were fraudulently

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

unlocked without AT&T's authorization or consent as a result of Defendants' scheme. AT&T will amend this complaint to allege the John Doe Defendants' true names and capacities when ascertained. AT&T will exercise due diligence to determine the John Doe Defendants' true names, capacities, and contact information to effect service upon the John Doe Defendants.

16. AT&T is informed and believes and thereupon alleges that each of the fictitiously named Doe Defendants is responsible in some manner for the occurrences herein alleged and that AT&T's injuries as herein alleged were proximately caused by such Defendants.

JURISDICTION AND VENUE

17. The Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331 because AT&T's claims for violations of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.* arise under federal law. The Court also has subject matter jurisdiction pursuant to 28 U.S.C. § 1332 because AT&T is a citizen of Delaware and Georgia, the Defendants are citizens of Washington and California, and this case involves claims exceeding $75,000 in damages, not including interest and costs. The Court has supplemental subject matter jurisdiction over AT&T's state law claims pursuant to 28 U.S.C. § 1367 because those claims are so related to the federal claims that they form part of the same case or controversy.

18. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(b) because a substantial part of the events or omissions giving rise to AT&T's claims occurred within this judicial district.

19. This Court has personal jurisdiction over the Defendants either by residence or because Defendants have conducted, engaged in, and carried out business ventures within the

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

state of Washington, have committed torts within or directed at the state of Washington, and have engaged in substantial and not isolated activity within the state of Washington.

FACTUAL BACKGROUND

AT&T'S BUSINESS AND SERVICES

20. AT&T is one of the nation's largest wireless carriers, with millions of subscribers using AT&T's wireless voice and data network.

21. AT&T enables customers to choose from a variety of monthly voice and data plans for use with devices on the AT&T wireless network. In addition to being available on AT&T's website and in its stores, AT&T phones and wireless services are sold through authorized AT&T dealers and retailers across the country.

22. AT&T's business model is based upon AT&T's ability to deliver an affordable and cutting edge product to its customers. At all times relevant to this Complaint, AT&T offered subsidies to its customers by selling the phones for substantially less than the phones cost AT&T to assist customers with the acquisition of AT&T phones. AT&T recouped this subsidy through profits earned on the sale of AT&T's wireless services, including calls, text messages, and transmission of data through AT&T phones. AT&T was able to offer its phones to customers at reduced prices because of the revenue AT&T generated when the phones were used as intended on the AT&T wireless network for the term of the contract.

23. AT&T's subsidy program was designed to ensure that AT&T customers have access to the newest technology, in order to provide customers with the best possible wireless service experience. Providing customers with the latest equipment also helps AT&T maintain the efficiency of its wireless network and facilitates the migration of customers from older technologies to newer products. AT&T offers new phones, upgraded with the latest

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

technology, to its customers at the inception of a new customer account and at various intervals during the customer's tenure.

24. Manufacturers that produce wireless phones for AT&T install proprietary locking software into AT&T phones. Among other things, this locking software prevents the phones from being used on any wireless network other than the AT&T network unless and until the phones are unlocked.

25. Like all wireless carriers in the United States, AT&T has policies in place to unlock phones for customers in certain circumstances. One example is when a customer wishes to use her phone for international travel.

26. The Wireless Customer Agreement entered into between AT&T and each of its customers also authorizes AT&T to effectuate the unlocking of a customer's phone upon the satisfaction of certain criteria. In 2013, AT&T customers were only permitted to unlock five phones per account per year under their Wireless Customer Agreements.

27. Defendants and others who improperly unlocked phones for the purpose of illicitly profiting from the resale of the unlocked phones were not authorized to do so.

DEFENDANTS' UNLOCK SCHEME

28. The practice of locking cell phones has been an essential part of the wireless industry's business model for many years and has been used by many major wireless providers.

29. Unlocked phones – which can be sold and used on any other compatible network anywhere around the world – are therefore a valuable commodity in secondary resale markets.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

30. The wireless industry has frequently fallen victim to large-scale phone trafficking operations in which illegal operators buy or steal large quantities of phones (pre-paid or with term contracts), unlock them, and resell them in foreign markets that do not subsidize the devices.

31. Accordingly and unfortunately, illicit bulk unlock schemes are not uncommon.

32. Defendants here engaged in just such a scheme.

A. AT&T's Discovery of Increased Unlock Requests

33. In 2013, AT&T employed Defendants Evans, Sapatin, and Lam as Customer Support Specialists in its Bothell, Washington Mobility Customer Care call center.

34. As Customer Care Support Specialists, Defendants Evans, Sapatin, and Lam had access to AT&T's computer systems in order to assist AT&T customers with service and billing issues. They also had the ability to submit unlock requests on behalf of eligible customers.

35. AT&T authorizes customer care personnel to utilize a web-based application, now referred to as "Torch," to research and troubleshoot customer service issues. Access to Torch is limited to authenticated users connected to AT&T's internal and protected corporate network.

36. In addition to resolving service and billing issues, Torch permits users with the proper authorization to, in appropriate circumstances, send requests to unlock the phones of AT&T customers.

37. Based on the credentials that users must provide to log into the Torch program, all unlocking transactions can be traced to the specific AT&T employee that sent the unlock request.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

38. On or around September 26, 2013, AT&T Asset Protection ("AP") personnel received information from the Torch technical support team that suggested abuse of the Torch program may have caused a recent surge in requests to unlock phones from AT&T's wireless network. AT&T AP personnel began an investigation into the potential compromise of the Torch program.

39. AT&T's investigation revealed that the employee credentials of Defendants Evans and Sapatin were associated with disproportionately large instances of use of Torch's "unlocking" function during the relevant time period.

40. AT&T's review of the unlock requests associated with Defendants Evans and Sapatin further revealed that the unlock requests occurred within milliseconds of one another, suggesting the use of an automated or scripted process to unlock devices, rather than manual submission of unlock requests in the ordinary course of business.

B. Defendant Evans's Participation in the Unlock Scheme

41. A review of Evans's computer by AT&T AP personnel revealed the presence of unusual and unauthorized malware programs.

42. "Malware" is a term that means "malicious software" and refers to software designed to damage or disable computers or computer systems.

43. The nature and characteristics of the malware files on Evans's computer indicated that she received and installed the files manually on AT&T's protected computer systems.

44. Once placed on AT&T's computer network by Evans, the malware permitted commands issued from a remote and unauthorized server, external to AT&T, to be communicated to the Torch program through Evans's infected computer. Through these

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

external commands, the malware program used valid customer service personnel identification numbers, including those of Defendants Evans, Sapatin, and Lam, to process automated unlock requests without AT&T's authorization.

45. Investigation of Evans's computer file activity during the relevant time period revealed that, from April to September 2013, Evans downloaded to and accessed from AT&T's protected computers numerous malware programs, which were intended to and actually did transmit or facilitate the transmission of fraudulent and unauthorized unlock requests through the Torch program, resulting in the unauthorized unlocking of thousands of phones on AT&T's wireless network.

46. The multiple malware programs downloaded and accessed by Evans progressed from early iterations, which gathered confidential and proprietary information on how internal AT&T applications worked, to the final version, which was ultimately unlocking thousands of AT&T devices per day through the compromised Torch program.

47. Upon information and belief, the early iterations of the malware programs gathered confidential and proprietary information regarding AT&T's internal applications and computer systems and transmitted that information to John Doe Defendants 1-50 through the remote server. The John Doe Defendants used that information to adjust the malware to specifically facilitate the hacking of the Torch application and then sent revised malware files to Evans for installation.

48. As a result of Evans's conduct, thousands of unauthorized and fraudulent unlock requests were transmitted under her employee identification number.

49. Evans's access to and/or execution of the malware programs was done intentionally, knowingly, and with intent to harm and defraud AT&T and was without

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

authorization by AT&T or in excess of her authorized access to AT&T's protected computer systems.

50. Defendant Vira, doing business as Swift Unlocks (together with Swift Unlocks, Inc., "Swift Unlocks"), paid Evans at least $20,000 for her placement and/or execution of the malware programs on AT&T's protected computer systems for the purpose of securing the fraudulent unlocks.

51. Evans took action to conceal or delete her fraudulent and unauthorized activities on AT&T computers.

52. In October 2013, Evans went on medical leave. She returned to work in February 2014, and was subsequently placed on administrative leave pending the outcome of AT&T's investigation into the Torch malware attack. Evans was directed to return to work on February 20, 2014, but declined to do so. She is no longer employed by AT&T.

C. Defendant Sapatin's Participation in the Unlock Scheme

53. Defendant Sapatin's employee credentials were associated with the largest number of unlock requests during the relevant time period. When AT&T AP personnel collected and reviewed Sapatin's computers in late September or early October 2013, many of the same malware programs present on Evans's computers were found on Sapatin's computers.

54. As with Evans's malware, the nature and characteristics of the malware files on Sapatin's computer indicated that he received and installed the files manually on AT&T's protected computer systems.

55. The investigation of Sapatin's file activity during the relevant time period revealed that, from April to October 2013, Sapatin downloaded to and accessed from AT&T's

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

protected computers numerous malware programs, which were intended to and actually did transmit or facilitate the transmission of fraudulent and unauthorized unlock requests through the Torch program, resulting in the unauthorized unlocking of thousands of phones on AT&T's wireless network.

56. As a result of Sapatin's conduct, thousands of unauthorized and fraudulent unlock requests were made under his employee identification number.

57. Sapatin's access and/or execution of the malware programs was done intentionally, knowingly, and with intent to harm and defraud AT&T and was without authorization by AT&T or in excess of his authorized access to AT&T's protected computer systems.

58. Upon information and belief, Swift Unlocks paid Sapatin at least $10,500 for his access and/or execution of the malware programs on AT&T's protected computer systems for the purpose of securing the fraudulent unlocks.

59. Sapatin took action to conceal or delete his fraudulent and unauthorized activities on AT&T computers.

60. After being interviewed by AT&T AP, Sapatin left the company in October of 2013, purportedly for unrelated reasons, and is no longer employed by AT&T.

D. Defendant Lam's Participation in the Unlock Scheme

61. During the investigation of Defendants Evans and Sapatin, AT&T AP personnel began monitoring the Internet Protocol ("IP") address of the remote server under external control that issued commands to the Torch program through the malware. During this monitoring, AT&T AP personnel observed Defendant Lam's computer connecting to the remote server.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

62. AT&T AP collected and reviewed Lam's computers in October of 2013. The same malware present on the computers of Evans and Sapatin was also found on Lam's computers.

63. As with Evans and Sapatin's malware, the nature and characteristics of the malware files on Lam's computer indicated that he received and installed the files manually on AT&T's protected computer systems.

64. AT&T AP personnel's October investigation of Lam's file activity revealed that, during September 2013, Lam downloaded to and accessed from AT&T's protected computers numerous malware programs, which were intended to and actually did transmit or facilitate the transmission of fraudulent and unauthorized unlock requests using the Torch program.

65. As a result of Lam's conduct, thousands of unauthorized and fraudulent unlock requests were made under his employee identification number.

66. Lam's access and/or execution of the malware programs was done intentionally, knowingly, and with intent to harm and defraud AT&T and was without authorization by AT&T or in excess of Lam's authorized access to AT&T's protected computer systems.

67. Lam took action to conceal or delete his fraudulent and unauthorized activities on AT&T computers.

68. As a result of AT&T's investigation into the Unlock Scheme, Lam was suspended and eventually terminated by AT&T. As with Sapatin and Evans, he is no longer employed by AT&T.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

E. Defendants Vira and Swift Unlocks, Inc.'s Participation in the Unlock Scheme

69. Prashant Vira, an individual doing business as Swift Unlocks, and/or Swift Unlocks, Inc., operates a well-known website that markets unlocking services for consumers using a wide variety of domestic and international wireless carriers, including AT&T.

70. The rates charged by Swift Unlocks vary by type of phone, carrier, and turnaround time required by the individual purchasing unlock services.

71. Swift Unlocks also allows individuals to become a reseller of its unlock services.

72. Upon information and belief, Swift Unlocks has paid individuals, including Defendants Evans and Sapatin, to illegally and without authorization unlock phones from the networks of various wireless carriers, including AT&T.

73. While the complete extent of Swift Unlocks's participation in the Unlock Scheme is not yet known, Swift Unlocks was actively involved in several integral parts of the conspiracy; specifically, providing Defendants Evans, Sapatin, and Lam with the malware that the former AT&T employees then installed and executed, without authorization or consent, on AT&T's protected computer systems and compensating Defendants Evans and Sapatin (and Lam, through Sapatin) for their illegal and unauthorized actions.

F. Defendants' Cooperation and Coordination in the Unlock Scheme

74. Upon information and belief, Defendants had an agreement and a conspiracy to profit from their unauthorized and fraudulent access, manipulation, and use of AT&T's protected computers to unlock hundreds of thousands of AT&T phones.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

75. The malware was developed for use in the Unlock Scheme by John Doe Defendants 1-50. Once the malware was placed on AT&T's protected computer systems by Defendants Evans, Sapatin, and Lam, the John Doe Defendants then issued commands from the remote and unauthorized external server through the infected computers of Defendants Evans, Sapatin, and Lam to improperly access the Torch program. The John Doe Defendants used confidential and proprietary information gathered and transmitted from the Torch application to specifically tailor the malware to attack and alter the Torch application to transmit hundreds of thousands of fraudulent and unauthorized unlock requests without AT&T's knowledge or consent.

76. Swift Unlocks and John Doe Defendants 1-50 provided Defendants Evans, Sapatin, and Lam with the malware that the former AT&T employees then installed and executed without authorization or consent on AT&T's protected computer systems. After their investigation into the potential compromise of the Torch program, which began on or around September 26, 2013, AT&T AP personnel, in late September and in October 2013, discovered this malware on the computers of Defendants Evans, Sapatin, and Lam.

77. The presence of the same malware specifically designed to attack AT&T's internal programs on the computers of Defendants Evans, Sapatin, and Lam reflects their cooperation and coordination with Swift Unlocks and John Doe Defendants 1-50 in effectuating the Unlock Scheme.

78. Upon information and belief, Swift Unlocks and John Doe Defendants 1-50 paid Defendants Evans, Sapatin, and Lam for their illegal and unauthorized placement of the malware on AT&T's protected computer systems and execution of that malware.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

79. Upon information and belief, John Doe Defendants 1-50 sold or otherwise benefitted from the unlocking of the phones effected by Defendants' fraudulent and unauthorized Unlock Scheme.

80. Upon information and belief, Sapatin recruited Defendants Evans and Lam to participate in the Unlock Scheme.

81. Sapatin also attempted to recruit other AT&T employees to participate in the Unlock Scheme. Sapatin told at least one other AT&T employee he was trying to recruit that he knew an individual that had paid to develop software designed to unlock phones. Sapatin told the AT&T employee that she only had to click on a link provided by someone else involved in the Unlock Scheme to download the software, and the program would run invisibly on his computer. Sapatin promised the employee that she would make $2,000 every two weeks through her participation in the Unlock Scheme.

82. Sapatin also stated that he had a friend who started working at AT&T specifically to further the Unlock Scheme. Upon information and belief, that friend is Defendant Lam.

83. Sapatin further stated that there were many people across the country participating in the Unlock Scheme and others like it against different wireless carriers. Upon information and belief, some of these individuals are the John Doe Defendants 1-50.

84. Defendant Sapatin incorporated two businesses in 2013, which were used in furtherance of Defendants' Unlock Scheme: Sapatin Enterprises Inc. and Sapatin Nguyen Enterprises, Inc.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

85. As a result of Defendants' intentional and coordinated conspiracy, AT&T suffered damage to its protected computer systems and impairment of the Torch program and data, and hundreds of thousands of phones on AT&T's network were illegally unlocked.

HARM CAUSED BY DEFENDANTS' MISCONDUCT

86. Defendants' misconduct has damaged the integrity and availability of AT&T's Torch program and the related data associated with the program and the unlocked phones. It has also damaged Defendants' computers infected with the malware.

87. Defendants' misconduct has caused AT&T to incur significant losses, including, but not limited to, the costs associated with investigating and responding to the malware attack, assessing the damage caused by the malware attack, and restoring and protecting the Torch program, the data associated with the program, and Defendants' infected computers.

88. Defendants' actions also harmed AT&T by depriving AT&T of the opportunity to recoup its subsidies on the sale of its phones and to earn profits by providing wireless service to legitimate AT&T customers on the unlocked phones.

89. Defendants' actions have also tarnished AT&T's reputation and goodwill.

COUNT I: COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030 (AGAINST ALL DEFENDANTS)

90. AT&T reasserts the allegations set forth in Paragraphs 1 – 89 as though fully set forth herein.

91. All computers used by Defendants without authorization or in excess of their authorized access, or to damage, impair, access, or traffic AT&T information, including, but not limited to, all servers, desktop computers, and laptop computers, were at all relevant times

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

used in interstate commerce and are protected computers under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030(e).

A. Violation of Section 1030(a)(4) of the CFAA

92. Defendants Evans, Sapatin, and Lam knowingly, and with intent to defraud, downloaded onto AT&T's protected computers and executed the malware programs designed to defraud AT&T's Torch program into unlocking phones on AT&T's wireless network without AT&T's knowledge or consent.

93. AT&T did not authorize Defendants Evans, Sapatin, and Lam to download and execute the malware.

94. Defendants' conduct, which was intended to and actually did defraud AT&T, exceeded their authorized access to AT&T's protected computer systems, as defined by Section 1030(e)(6) of the CFAA.

95. Downloading the malware onto AT&T's protected computer systems and executing that malware was an integral part of the fraudulent Unlock Scheme and in fact furthered that scheme. As a result of their participation in this scheme, Defendants Evans, Sapatin, and Lam obtained information regarding AT&T's internal applications, secured the unlocking of hundreds of thousands of phones on AT&T's network, and received cash consideration, all of which are things of value.

96. By providing Defendants Evans, Sapatin, and Lam with the malware specially designed to attack AT&T's protected computer systems and compensating Defendants for downloading that malware onto AT&T's protected computer systems, Swift Unlocks and John Doe Defendants 1-50 knowingly, intentionally, and with the intent to defraud, facilitated the unauthorized access of AT&T's protected computer networks.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

97. As a result of their participation in this scheme, Swift Unlocks and John Does 1-50 at a minimum obtained information regarding AT&T's internal applications and secured the unlocking of hundreds of thousands of phones on AT&T's network, both of which are things of value.

98. Accordingly, the conduct of all Defendants constitutes unauthorized access of AT&T's protected computer systems in violation of Section 1030(a)(4) of the CFAA.

B. Violation of Section 1030(a)(5)(A) of the CFAA

99. Defendants knowingly caused the transmission of the malware, which constitutes a program, code, or command under Section 1030(a)(5)(A) of the CFAA, onto AT&T's protected computer systems.

100. By downloading and executing the malware on AT&T's protected computer systems, Defendants Evans, Sapatin, and Lam knowingly caused the transmission of the malware and intentionally caused damage to AT&T's protected computer systems.

101. By providing Defendants Evans, Sapatin, and Lam with the malware specially designed to attack AT&T's protected computer systems and compensating Defendants for downloading that malware onto AT&T's protected computer systems, Swift Unlocks and John Doe Defendants 1-50 knowingly caused the transmission of the malware to AT&T's protected computer systems without authorization from AT&T and intentionally caused damage to AT&T's protected computer systems.

102. AT&T did not authorize Defendants to transmit the malware onto AT&T's protected computer systems. Defendants' transmission was without AT&T's knowledge or consent.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

103. Accordingly, the conduct of all Defendants constitutes unauthorized transmission of a program, information, code, or command in violation of Section 1030(a)(5)(A) of the CFAA.

C. Violation of Section 1030(a)(5)(C) of the CFAA

104. Defendants Evans, Sapatin, and Lam intentionally accessed AT&T's protected computers to download onto them the malware programs designed to defraud AT&T's Torch program into unlocking phones on AT&T's wireless network without AT&T's knowledge or consent. AT&T did not authorize Defendants Evans, Sapatin, and Lam to download and execute the malware.

105. The conduct of Defendants Evans, Sapatin, and Lam caused damage to AT&T's protected computers infected with the malware, as well as to the Torch application and the data associated therewith, and loss to AT&T.

106. Accordingly, the conduct of Defendants Evans, Sapatin, and Lam constitutes unauthorized access of AT&T's protected computer systems in violation of Section 1030(a)(5)(C) of the CFAA.

D. Facts Common to All Violations

107. All Defendants knowingly and intentionally conspired to commit the offenses detailed above.

108. Defendants' unauthorized and fraudulent use of AT&T's protected computer systems has caused AT&T to suffer injury, with "damages" and "losses" – as those terms are defined in Sections 1030(e)(8) and 1030(e)(11), respectively – substantially in excess of $5,000 over a one-year period.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

109. With respect to damage, by infecting AT&T's protected computer systems with malware, Defendants have damaged and substantially impaired the integrity of the Torch program, its related data, and the computers infected by the malware in an amount in excess of $5,000 over a one-year period. Defendants' actions have also deprived AT&T of the means to control the quality of its products and services.

110. With respect to loss, Defendants' actions have caused AT&T to spend well in excess of $5,000 in a one-year period investigating and assessing the possible impairment to the integrity of its protected computer systems, taking action to counteract Defendants' conduct, conducting a damage assessment regarding the myriad effects of the malware infection, and restoring and protecting the Torch program. Defendants' conduct also deprived AT&T of its subsidy investment in its phones and caused AT&T loss of revenue and goodwill.

111. Because Defendants' conduct involves at least one of the factors identified in Section 1030(c)(4)(A)(i), and for the reasons set forth above, AT&T is entitled to assert this civil action to obtain compensatory damages and injunctive relief pursuant to 18 U.S.C. § 1030(g).

COUNT II: BREACH OF THE DUTY OF LOYALTY (AGAINST EVANS, SAPATIN, AND LAM)

112. AT&T reasserts the allegations set forth in Paragraphs 1 – 89 as though fully set forth herein.

113. At all times relevant to this Complaint, Defendants Evans, Sapatin, and Lam were employees of AT&T.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

114. As employees of AT&T, Defendants Evans, Sapatin, and Lam had a duty of loyalty to AT&T.

115. By improperly using AT&T's property and confidential information for their own benefit and for the benefit of Swift Unlocks and John Doe Defendants 1-50, Defendants Evans, Sapatin, and Lam acted against the best interests of their employer, AT&T.

116. By downloading and executing the malware, which was designed and intended to defraud AT&T, on AT&T's protected computer systems, Defendants Evans, Sapatin, and Lam acted against the best interests of their employer, AT&T.

117. By failing to disclose the Unlock Scheme to AT&T, Defendants Evans, Sapatin, and Lam acted against the best interests of their employer, AT&T.

118. By accepting undisclosed payments from Swift Unlocks for downloading and executing the malware on AT&T's protected computer systems, Defendants Evans, Sapatin, and Lam acted against the best interests of their employer, AT&T..

119. Through the above-stated conduct, as well as that set forth in Paragraphs 1-89, Defendants Evans, Sapatin, and Lam breached their duty of loyalty to AT&T.

120. Defendants Evans, Sapatin, and Lam's breach of their duty of loyalty to AT&T proximately caused AT&T damages in an amount to be determined at trial.

COUNT III: TORTIOUS INTERFERENCE WITH CONTRACT OR BUSINESS EXPECTANCY (AGAINST ALL DEFENDANTS)

121. AT&T reasserts the allegations set forth in Paragraphs 1 – 89 as though fully set forth herein.

122. AT&T has contractual relationships with its customers, which are governed by AT&T's Wireless Customer Agreements.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

123. In 2013, these contracts authorized unlocking of phones on AT&T's wireless network only in certain circumstances and limited unlocking to five phones per account per year under their Wireless Customer Agreements.

124. As then-employees of AT&T, Defendants Evans, Sapatin, and Lam were aware of the existence of AT&T's contracts with its customers and the requirements for unlocking phones on AT&T's wireless network. Upon information and belief, Swift Unlocks and John Doe Defendants' 1-50 were also aware of AT&T's customer contracts due to the nature of Swift Unlocks's business and through the Unlock Scheme.

125. By unlocking the phones of customers who may have otherwise been ineligible to unlock those phones through the use of unauthorized malware intended to defraud AT&T, Defendants intentionally interfered with AT&T's customer contracts through improper means and for an improper purpose, thereby causing a breach of those contracts and a loss of AT&T's expectancy in future business with those customers.

126. Defendants' tortious conduct proximately caused AT&T damages in an amount to be determined at trial.

COUNT IV: UNJUST ENRICHMENT (AGAINST DEFENDANT JOHN DOES 1-50)

127. AT&T reasserts the allegations set forth in Paragraphs 1 – 89 as though fully set forth herein.

128. By reselling phones unlocked fraudulently and without authorization pursuant to the Unlock Scheme, Defendant John Does 1-50 have received economic benefits acquired at AT&T's expense.

129. Defendants John Does 1-50 have acquired these benefits voluntarily and with full knowledge of the benefits.

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

130. Defendants John Does 1-50 have retained the benefits under such circumstances that make it unjust and inequitable for Defendant John Does 1-50 to retain such benefits without paying AT&T the value of the benefits Defendant John Does 1-50 acquired.

131. Accordingly, Defendants John Does 1-50 should disgorge their unjustly received gains in an amount to be determined at trial.

COUNT V: CIVIL CONSPIRACY

132. AT&T reasserts the allegations set forth in Paragraphs 1 – 89 as though fully set forth herein.

133. An agreement and conspiracy existed between and among the Defendants and other co-conspirators to unlawfully defraud AT&T by unlocking AT&T phones via the use of unauthorized malware on AT&T computers, which resulted in violations of the CFAA, tortious interference with contract, and unjust enrichment to Defendants, among other things.

134. Each Defendant intentionally participated in the agreement and conspiracy.

135. Each Defendant knowingly agreed to engage, and did engage, in one or more overt acts in pursuit of the conspiracy as set forth with particularity above.

136. AT&T has been proximately damaged by the conspiracy and Defendants' actions in furtherance thereof.

DEMAND FOR JURY TRIAL

137. AT&T demands a trial by jury on all triable issues.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff AT&T Mobility LLC respectfully requests that the Court enter final judgment in favor of AT&T and against Defendants as follows:

K&L GATES LLP
925 FOURTH AVENUE
SUITE 2900
SEATTLE, WASHINGTON 98104-1158
TELEPHONE: (206) 623-7580
FACSIMILE: (206) 623-7022

(a) Awarding AT&T its compensatory, consequential, and special damages including, without limitation, its lost profits, lost goodwill and damage to its reputation, and Defendants' profits, together with pre and post-judgment interest, as provided by law;

(b) Awarding AT&T its reasonable attorneys' fees and costs associated with this action;

(c) Granting permanent injunctive relief in favor of AT&T and against Defendants enjoining Defendants from engaging in the unlawful practices described in this Complaint; and

(d) Granting such further relief as this Court deems just and proper.

Respectfully submitted this 11th day of September, 2015.

/s/ David A. Bateman
David Bateman, WSBA #14262
K&L GATES LLP
925 Fourth Avenue, Suite 2900
Seattle, WA 98104-1158
Phone: (206) 370-6682
david.bateman@klgates.com

David L. Balser, Georgia Bar No. 035835
(pro hac vice application forthcoming)
Claire C. Oates, Georgia Bar No. 702045
(pro hac vice application forthcoming)
KING & SPALDING LLP
1180 Peachtree St. NE
Atlanta, Georgia 30309-3521
Tel: (404) 572-4600
Fax: (404) 572-5100

Counsel for Plaintiff
AT&T Mobility LLC