UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
CASE NO: 9:19-cv-81160-RS

APPLE INC.,

Plaintiff,

v.

CORELLIUM, LLC,

Defendant.

_____/

CORELLIUM'S ANSWER, AFFIRMATIVE DEFENSES, AND COUNTERCLAIMS

Defendant, Corellium, LLC ("Corellium" or "Defendant"), by and through its undersigned counsel, files its Answer, Affirmative Defenses, and Counterclaims to Plaintiff, Apple Inc.'s ("Apple" or "Plaintiff") Complaint:

RELEVANT BACKGROUND

Long before Apple accused Corellium of copyright infringement, Apple not only encouraged Corellium to continue developing its technology, [redacted]. During this time, Apple approved of Corellium participating in its invitation-only Security Bounty Program ("bug bounty program") with a promise to pay for software bugs identified by Corellium. While Apple gladly accepted and utilized bugs submitted by Corellium as part of this program, it broke its promise to pay for them. Finally, [redacted], Apple announced its own competing product and soon after sued Corellium. Tellingly, [redacted]

[redacted], Apple never hinted that it believed Corellium was infringing its copyrights.

Apple's behavior with respect to security research is widely viewed as harmful to the public. By way of example, Apple's behavior toward Corellium exemplifies its desire to exclusively control the manner in which security researchers identify vulnerabilities in, e.g., a mobile device's operating system. This research is extremely important to the public's interest. By requiring that security researchers use its physical development ("dev") devices to the exclusion of other products, including its attempt to stop Corellium from offering a more efficient alternative to its dev devices, Apple is trying to exclusively control (1) how security research is performed, and (2) who is able to perform that research.

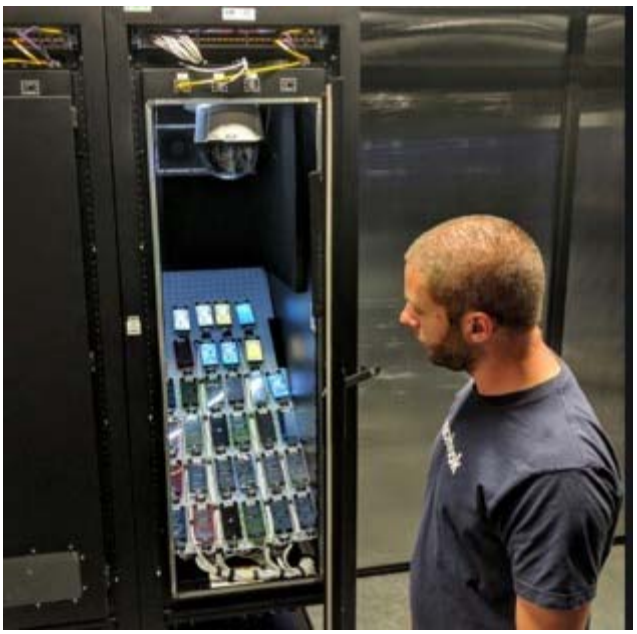
In view of the foregoing, this lawsuit is not driven by Apple's genuine belief that Corellium infringes its copyrights, [redacted]. Apple's behavior, which spans the course of several years and has culminated in filing this lawsuit, amounts to unfair business practices that must be put to an end by the Court.

Corellium's Innovative And Transformative Technology Has Transformed Security Research

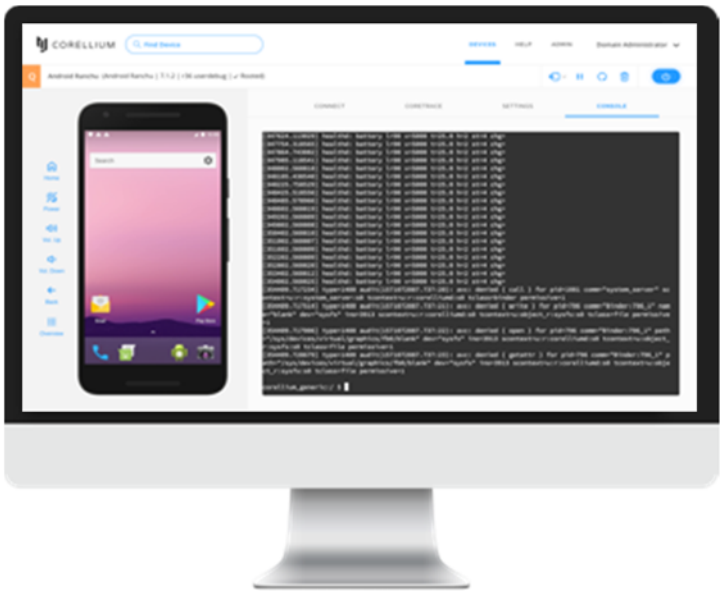
[redacted] Corellium's technology because it is innovative and highly transformative. It virtualizes physical devices, including Apple mobile devices, enabling users to execute various device operating systems in a simple unified environment. By replacing racks of physical devices[1] with a single virtual platform, Corellium empowers software engineers to test, teach, research, and develop more efficiently and more effectively.

[1] *See, e.g.*, Frederic Lardinois, *Facebook Lifts The Veil On Its Mobile Device Testing Lab*, TECHCRUNCH (July 13, 2016), https://techcrunch.com/2016/07/13/facebook-lifts-the-veil-on-its-mobile-device-lab/ (noting the way in which Facebook tests changes to its smartphone application).

BEFORE CORELLIUM



AFTER CORELLIUM



Corellium's technology provides a substantially more scalable, convenient, and efficient solution than the status quo. For example, using Corellium's technology, security researchers and

developers can quickly search for errors and vulnerabilities ("bugs") in an application ("app") or operating system across multiple device models and operating system versions and write programs to automate these tasks. Similarly, if a bug "bricks" a virtual device and renders it unusable, a security researcher can instantly generate a new virtual machine rather than obtain a new physical device. This is one of several examples where Corellium's technology is more efficient than the use of physical devices to perform security research.

Corellium's technology is not only more efficient, but also provides new and advanced functionality that is more effective than a physical device. For example, Corellium's technology allows a virtual device to be paused during testing, which gives researchers a detailed look at its state at any given moment.

Given the benefits of Corellium's technology, it is no wonder third-party security experts have endorsed Corellium's technology:

> "Corellium was founded in Florida in 2017, in the last two years it has earned a ***sterling reputation*** among mobile jail breakers and cybersecurity specialists . . . ." [2]
>
> "Its product provides 'virtualized' versions of iOS. For security researchers, such software-only versions of the Apple operating system are ***incredibly valuable***. For instance, it's possible to use Corellium to pause the operating system and analyze what's happening at the code level. ***Some in the industry have called it 'magic,'*** as it should help security researchers uncover vulnerabilities with greater ease and speed than having to work with a commercial iPhone."[3]
>
> "You are obviously all from other planets as there is NO WAY in hell this was made by humans. Alien tech and I for one welcome our new overlords. ***This is magic and truly will change stuff***. The sheer flexibility to virtualise the downgrading of devices, to test fixes/bugs/features on older versions, is

[2] Conor Reynolds, *Apple Sues Virtualization Firm Corellium for "Perfect Digital Facsimile" of iOS*, COMPUTER BUSINESS REVIEW (Aug. 16, 2019), https://www.cbronline.com/news/apple-sues-corellium (emphasis added).

[3] Thomas Brewster, *Apple Sues Cybersecurity Startup for 'Illegally Replicating' iPhone for iOS*, FORBES (Aug. 15, 2019), https://www.forbes.com/sites/thomasbrewster/2019/08/15/apple-is-suing-a-cybersecurity-startup-for-illegally-replicating-iphones/#7d0ff994522b (emphasis added).

> amazing. Then, ability to change Device IDs on the fly, with Coretrace, this is heaven."[4]

At bottom, Corellium's technology is innovative and transformative, [redacted], Apple is now attempting to use the court system to shut it down.

Further, Corellium has made quintessential fair use of Apple's technology. Corellium's technology is highly transformative because it does not merely replicate Apple's products for the same purposes for which the products were developed. Instead, Corellium's technology utilizes portions of Apple's technology for entirely distinct purposes, which provide significant societal benefits. For example, a user of Corellium's technology cannot perform most functions that make a smartphone attractive: a user cannot make phone calls or send text messages. Nor can a user access iTunes, log into an iCloud account, navigate with GPS, pair Bluetooth headphones, or take pictures. Instead, a user of Corellium's technology is constrained to use Apple's technology for the purposes of, e.g., research, testing, and development. In other words, Corellium's highly transformative use of Apple's technology is for an entirely distinct purpose – research and improving the operating system itself – rather than the purposes for which Apple designed its products. And the purpose of using Corellium's technology has significant societal value, i.e., the types of benefits the fair use doctrine is specifically meant to encourage.

It follows that Corellium does not use iOS in its entirety or merely replicate iOS for the same purposes as Apple. Instead, Corellium uses its own proprietary software to facilitate executing iOS on different hardware. When iOS is loaded onto the Corellium platform, it is not

---

[4] Daniel Cuthbert (@dcuthbert), TWITTER (Aug. 14, 2019), https://twitter.com/dcuthbert/status/1161650762142887936?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1161650762142887936&ref_url=https%3A%2F%2Fpublish.twitter.com%2F%3Fquery%3Dhttps%253A%252F%252Ftwitter.com%252Fdcuthbert%252Fstatus%252F1161650762142887936%26widget%3DTweet (emphasis added).

only transformed to enable it to run on different hardware, but it is also integrated with third-party tools to improve the utility of the platform for developers. Apple cannot dispute that Corellium implements its own original code and virtual machine in conjunction with third party tools. And, while Apple is forced to rely upon physical devices to identify vulnerabilities or test new apps, Corellium's technology enables iOS to run on a virtual platform – thereby obviating several limitations associated with using physical devices to perform such tasks. [redacted].

Because Corellium's technology is highly transformative, it cannot reasonably be said to harm the market for Apple's products. Apple cannot be genuinely concerned it will lose smartphone market share to Corellium, because Corellium's technology is in no way a market substitute for Apple's products. Corellium's technology simply has no relevant impact on Apple's position in the marketplace. Apple does not (and cannot) plead otherwise.

Apple's Attempts To Purchase Corellium's Predecessor Company—Virtual, LLC

Unsurprisingly, Apple's Complaint omits key information about Apple's lengthy relationship with Corellium, its technology, and its founders. Apple has long admired Corellium's founders and tried to recruit them [redacted] for several years.

In 2011, Corellium co-founder Chris Wade developed and launched iEmu, an open-source iOS emulator that emulated iOS applications on Android, Mac, and Windows devices.[5] When Mr. Wade discussed his emulator with Apple's Head of Security Engineering and Architecture, Ivan Krstić, Mr. Krstić called the emulator "awesome" and requested that Mr. Wade send him a "paragraph or two about what it supports and how far you've gotten" that Mr. Krstić could "pass around." At that time, Mr. Krstić also tried to recruit Mr. Wade to join Apple for Mr. Krstić's

[5] *iEmu: an open-source iOS device emulator*, KICKSTARTER.COM (Aug. 16, 2011), https://www.kickstarter.com/projects/cmwdotme/iemu-an-open-source-ios-device-emulator.

self-proclaimed "totally selfish motive of working with the smartest people in the world."

However, Mr. Wade did not join Apple. Instead, he, Amanda Gorton, and Stanislaw Skowronek developed and launched their first virtualization platform for iOS devices in 2014 called Virtual, LLC ("Virtual"). The technology offered by Virtual is similar to the technology offered by Corellium. [redacted]. The team decided to sell their company to Fort Lauderdale-based Citrix [redacted].

[redacted]

[redacted]

[redacted]

[redacted]

Apple's Use Of Corellium's Technology

[redacted] it also approved Corellium to participate in its invitation-only bug bounty program, a program in which Mr. Wade had already been participating for more than a year. Through this program, Apple pays security researchers to submit bugs they find in Apple's operating systems to Apple. While Corellium has submitted several bugs, Apple has failed to pay Corellium for any of them. Why? The reason is simple: [redacted]

Due to Apple's refusal to pay, it is Apple that owes Corellium. Rather than paying Corellium, Apple is now trying to get additional bugs from the company for free. Apple's First Set of Requests for Production requests Corellium to provide Apple with "any bugs, exploits, vulnerabilities, or other software flaws in iOS of which Corellium or its employees currently ***are, or have ever been, aware***" (emphasis added). Through this lawsuit, Apple continues its practice of obtaining and retaining the benefit of Corellium's technology without paying for the benefits it received.

[redacted] Apple Offered A New Product To Compete With Corellium's Technology

Just days before filing this lawsuit, Mr. Krstić announced at the Black Hat USA conference that Apple would increase the maximum reward amounts available for bug bounty submissions

from $200,000 to $1,000,000 and also open up the bug bounty program to anyone interested in participating. Mr. Krstić also announced that Apple would give select independent security researchers special "pre-hacked" research devices so that they can search for flaws in the iOS.[6]

While Apple's announcement was originally seen as a gesture of goodwill by a company that has been notoriously hostile to security researchers, it is clear from this lawsuit that Apple's announcement was just that, a gesture. Corellium's technology does what Apple clearly wants to prohibit any entity from doing – open up the security research and application development fields to third parties. Why else would Apple introduce new exclusive devices for security researchers and then – within days – file this lawsuit against Corellium? To stifle competition by preventing Corellium from offering third party researchers a more efficient alternative. Indeed, Apple's Complaint acknowledges "that a cloud-based product like Corellium's will compete directly with the custom devices that Apple plans to distribute to security researchers." Doc. 1, ¶ 40. Through its invitation-only research device program and this lawsuit, Apple is trying to control who is permitted to identify vulnerabilities, if and how Apple will address identified vulnerabilities, and if Apple will disclose identified vulnerabilities to the public at all.

Apple's Real Reason For Suing Corellium

So why did Apple sue Corellium? [redacted] Apple was not only aware of Corellium's technology for several years, but actually encouraged its development.

[6] Lorenzo Francecshi-Bicchierai, *Apple's Lawsuit Against a Startup Shows How It Wants to Control the iPhone Hacking Market*, VICE NEWS (Aug. 16, 2018), https://www.vice.com/en_us/article/d3a8jq/apple-corellium-lawsuit.

Rather than tell the real story, Apple paints Corellium as a bad actor, unscrupulously peddling its product to anyone for any reason. But Corellium does not license its platform to anyone. Its end users include well-known and well-respected financial institutions, government agencies, and security researchers. Financial institutions use Corellium's technology to test their mobile banking apps to make them impenetrable to hackers and ensure stability in the event of heavy traffic. Government agencies use Corellium's technology for the purpose of national defense. Security researchers use Corellium's technology to more efficiently and effectively search for and repair security vulnerabilities in, e.g., mobile device apps and services.

Further, the founders of Corellium's first customer, Azimuth Security ("Azimuth"), wrote the book on security research: "The Art of Software Security Assessment." Azimuth is owned by L3 Harris Technologies, Inc. ("L3") – a government contractor headquartered in Melbourne, Florida, known for its space and defense communications systems. Contrary to Apple's disparaging implication, Corellium and its founders do business with those working in software security to protect end users – not use it for an improper purpose.

Corellium's Technology Advances The Public Interest

Soon after Apple sued Corellium, security researchers at Google's Project Zero identified and disclosed a hacking campaign that exploited five distinct iOS exploit chains by embedding attacks in certain websites. Specifically, the press reported that flaws in Apple's iOS security allowed the Chinese government to target Uyghur Muslim minorities by infecting their iPhones with malicious code that allowed attackers to read text messages, obtain passwords, and track locations in near-real time.[7] It also infected the phones of non-Uyghurs and forced the FBI to ask

[7] Zach Whittaker, *Sources say China used iPhone hacks to target Uygur Muslims*, TECHCRUNCH (Aug. 31, 2019), https://techcrunch.com/2019/08/31/china-google-iphone-uyghur/.

Google to de-index the offending websites in order to reduce the number of infections.[8]

Apple was forced to publicly admit the Uyghurs were attacked as a result of these iPhone security flaws, but disputed certain other information provided by Google.[9] Although Google and Apple are fierce rivals in the smartphone market, Google's Project Zero (like Corellium) is focused on finding and fixing security flaws in a wide range of software and hardware firms, not just Apple.

According to a recent press article, Apple's security flaws indicate:

> Cupertino still has work to do in safeguarding its devices and services and it's time for the company to deeply examine its own software for issues that resulted in the flaws that've made those iPhone attacks possible.[10]

Corellium agrees. Corellium's technology is intended to improve the security research and development community. Apple's copyrights were never intended to cover or apply to Corellium's technology. The Copyright Act is simply not that broad. *See* 17 U.S.C. § 102(b). Perhaps if Apple focused more on security and less on litigation, it would not suffer the security flaws identified in recent press reports.

CORELLIUM'S ANSWER TO APPLE'S COMPLAINT

1. Corellium admitts that Apple initated this lawsuit, but denies any liablity or wrongdoing and denies that Apple is entitled to any relief.

INTRODUCTION

2. Denied.

3. Denied.

---

[8] Ravie Lakshmanan, *iPhone Spyware Campaign Reportedly Targeted Uyghur Muslims For 2 Years*, THE NEXT WEB (Sept. 6, 2019), https://thenextweb.com/security/2019/09/02/iphone-spyware-campaign-reportedly-targeted-uyghur-muslims-for-2-years/.

[9] Stephen Nellis, *Apple Says Uighurs Targeted In iPhone Attack But Disputes Google Findings*, REUTERS (Sept. 6, 2019), https://www.reuters.com/article/us-apple-cyber/apple-says-uighurs-targeted-in-iphone-attack-but-disputes-google-findings-idUSKCN1VR29K.

[10] Lakshmanan, *supra* note 8.

4. Denied.

5. Denied.

6. Denied.

7. Denied.

THE PARTIES

8. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 8, and therefore denies same.

9. Corellium admits that it is a limited liability company registered in Delaware. Corellium denies the remaining allegations in paragraph 9.

JURISDICTION AND VENUE

10. Admitted.

11. Admitted.

12. Admitted.

FACTS COMMON TO ALL CLAIMS FOR RELIEF

A. Apple's Copyrighted Works

13. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 13, and therefore denies same.

14. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 14, and therefore denies same.

15. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 15, and therefore denies same.

16. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 16, and therefore denies same.

17. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 17, and therefore denies same.

18. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 18, and therefore denies same.

19. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 19, and therefore denies same.

20. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 20, and therefore denies same.

21. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 21, and therefore denies same.

22. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 22, and therefore denies same.

B. Corellium's Infringing Product

23. Denied.

24. Denied.

25. Denied.

26. Denied.

27. Denied.

28. Denied.

29. Denied.

30. Denied.

31. Denied.

32. Denied.

33. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 33, and therefore denies same.

34. Corellium admits that the statements referenced in paragraph 34 purport to be attributable to Mr. Wade. The statements speak for themselves, and Corellium denies the allegations contained in paragraph 34 to the extent Apple attempts to characterize same.

35. Corellium admits that Mr. Wade appeared on a podcast called Risky Business. Corellium admits that the statements referenced in paragraph 35 purport to be attributable to Mr. Wade. The statements speak for themselves, and Corellium denies the allegations contained in paragraph 35 to the extent Apple attempts to characterize same.

36. Denied.

37. Denied.

38. Denied.

39. Denied.

40. Denied.

41. Denied.

C. Corellium's Acts of Copyright Infringment

42. Denied.

43. Denied.

44. Denied.

FIRST CLAIM FOR RELIEF

Direct Federal Copyright Infringment (Computer Programs), 17 U.S.C. § 501

45. Corellium realleges and incorporates by reference each of the answers and responses in preceding paragraphs 1-44 set forth above.

46. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 46, and therefore denies same.

47. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 47, and therefore denies same.

48. Denied.

49. Denied.

50. Denied.

51. Denied.

SECOND CLAIM FOR RELIEF

Direct Federal Copyright Infringment
(Graphical User Interface Elements), 17 U.S.C. § 501

52. Corellium realleges and incorporates by reference each of the answers and responses in preceding paragraphs 1-51 set forth above.

53. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 53, and therefore denies same.

54. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 54, and therefore denies same.

55. Denied.

56. Denied.

57. Denied.

58. Denied.

THIRD CLAIM FOR RELIEF

Contributory Federal Copyright Infringment, 17 U.S.C. § 501

59. Corellium realleges and incorporates by reference each of the answers and responses in preceding paragraphs 1-58 set forth above.

60. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 60, and therefore denies same.

61. Denied.

62. Denied.

63. Denied.

64. Denied.

PRAYER

Corellium denies that Apple is entitled to any relief whatsoever including, but not limited to, equitable, injunctive, compensatory, or punitive relief, and requests that the Court dismiss all claims against Corellium with prejudice and order such further relief as the Court deems just and proper.

CORELLIUM'S AFFIRMATIVE DEFENSES

By asserting its Affirmative Defenses, Corellium does not agree or concede that it bears the burden of proof or the burden of persuasion on any of these issues, whether in whole or in part. Corellium reserves the right to add or amend its defenses further as additional information is developed through discovery or otherwise. Corellium sets forth the following affirmative defenses:

FIRST AFFIRMATIVE DEFENSE
(Failure to State a Claim)

1. For its first affirmative defense, Corellium states that Apple's claims are barred, in whole or in part, because Apple fails to state a claim against Corellium upon which relief can be granted.

SECOND AFFIRMATIVE DEFENSE
(Fair Use)

2. For its second affirmative defense, Corellium states that any alleged violation of Apple's alleged copyright protections is permissible under the doctrine of fair use. Specifically, the purpose of Corellium's product is for, *inter alia*, the criticism, research, and/or improvement of Apple's alleged copyright-protected material. Further, Corellium's use of any of Apple's copyright-protected material is transformative in nature such that any action on the part of Corellium does not constitute infringement or any other violation of a law or right.

THIRD AFFIRMATIVE DEFENSE
(Estoppel)

3. For its third affirmative defense, Corellium states that Apple is not entitled to its requested relief under the doctrine of estoppel. Apple is estopped from seeking the requested relief as the position taken by Apple in this case is contrary to a prior position taken by Apple. It has been aware of Corellium's technology but failed to seek any legal recourse or otherwise object to Corellium's actions. Instead, Apple encouraged the continued development of Corellium's technology.

FOURTH AFFIRMATIVE DEFENSE
(Laches)

4. For its fourth affirmative defense, Corellium states that Apple is not entitled to its requested relief under the doctrine of laches. Corellium states that Apple is estopped from seeking

the requested relief as Apple has been long-aware of Corellium's technology but failed to seek any legal recourse or otherwise object to Corellium's actions.

FIFTH AFFIRMATIVE DEFENSE
(Waiver)

5. For its fifth affirmative defense, Corellium states that Apple is not entitled to its requested relief under the doctrine of waiver. Corellium states that Apple has waived its rights to any sought relief because Apple has been aware of Corellium's technology but failed to seek any legal recourse or otherwise object to Corellium's actions. Instead, Apple encouraged the continued development of Corellium's technology.

SIXTH AFFIRMATIVE DEFENSE
(Unclean Hands)

6. For its sixth affirmative defense, Corellium states that Apple is not entitled to its requested relief under the doctrine of unclean hands. Apple acknowledged and understood Corellium's existence and operations, but failed to seek any legal recourse or otherwise object to Corellium's actions. Instead, Apple encouraged the continued development of Corellium's technology.

SEVENTH AFFIRMATIVE DEFENSE
(Restraint of Trade)

7. For its seventh affirmative defense, Corellium states that a finding of infringement would be contrary to public policy and business innovation and would constitute a restraint of trade. Specifically, the public has an interest in free markets, competition, and secure and robust software. Corellium denies any violation of any law or right, and states that its business and the products it provides promote competition and encourage secure and robust software by developing a platform that eases the access to such software to those that can research and improve upon same.

EIGHTH AFFIRMATIVE DEFENSE
(Authorized Use, License, Consent, Acquiescence)

8. For its eighth affirmative defense, Corellium states that Apple is not entitled to its requested relief under the doctrine of acquiescence. Apple's claims are barred, in whole or in part, by license or the doctrine of implied license because Apple impliedly, directly, or indirectly, authorized, licensed, consented to, or acquiesced to Corellium's allegedly infringing use of Apple's works.

NINTH AFFIRMATIVE DEFENSE
(Invalidity or Unenforceablity of Copyright)

9. For its ninth affirmative defense, Corellium states that Apple's applicable copyright registrations are invalid, in whole or in part, and/or Apple is otherwise attempting to exceed the scope of its registrations in that Apple seeks to protect unprotectable information, such as, *inter alia*, facts, the functionality of software components, or other public information.

TENTH AFFIRMATIVE DEFENSE
(*Scenes a Faire* Doctrine)

10. For its tenth affirmative defense, Corellium states that Apple's claims are barred, in whole or in part, because critical parts or portions of Apple's alleged protected copyrights are invalid due to consisting of unprotectable *scenes a faire*. Specifically, elements of Apple's copyrighted works are dictated by practical realities, such as by hardware standards and mechanical specifications, software standards and compatability requirements, as well as standard programming practices, and may not obtain copyright protection as such.

ELEVENTH AFFIRMATIVE DEFENSE
(Merger Doctrine)

11. For its eleventh affirmative defense, Corellium states that Apple's claims are barred, in whole or in part, by the doctrine of merger. Specifically, the ideas underlying Apple's

copyrighted works can only be expressed in certain limited ways, such that they are inseparably tied to their on-screen expression. In sum, there is merger of idea and expression.

TWELFTH AFFIRMATIVE DEFENSE
(No Willful Infringement)

12. For its twelfth affirmative defense, Corellium states that its actions were in good faith and with non-willful and innocent intent at all material times. Apple's claims to enhanced damages and an award of fees and costs against Corellium are barred because they have no basis in fact or law.

THIRTEENTH AFFIRMATIVE DEFENSE
(Misuse)

13. For its thirteenth affirmative defense, Corellium states that Apple is not entitled to its requested relief under the doctrine of misuse. Apple is attempting to use its alleged copyright protections for an impermissible purpose. For example, Apple is attempting to limit and obstruct innovation, trade, and commercial activity. Apple is thereby exceeding the scope of its permissible copyright protection.

FOURTEENTH AFFIRMATIVE DEFENSE
(*De Minimis* Infringement)

14. For its fourteenth affirmative defense, Corellium states that Apple's claims for copyright infringement against Corellium are barred by the doctrine of *de minimis* copying where Corellium's alleged use of any protectable portions of the works that are the subject of the asserted copyrights, if any, is *de minimis*.

FIFTEENTH AFFIRMATIVE DEFENSE
(Innocent Intent)

15. For its fifteenth affirmative defense, Corellium states that it justifiably relied upon the actions, statements, praise, and/or encouragement from Apple in the operation of its business and development of its product.

16. Corellium states that discovery is still ongoing and reserves the right to amend its Answer and Affirmative Defenses and add additional defenses or avoidances, pursuant to Fed. R. Civ. P. 8, as they may become known through the discovery process

COUNTERCLAIMS AGAINST APPLE

Corellium brings the following Counterclaims against Plaintiff/Counter-Defendant Apple Inc. ("Apple") and alleges as follows:

THE PARTIES

1. Corellium is a Delaware limited liability company incorporated under the laws of Delaware with its principal place of business at 1301 N Congress Ave, Suite 410, Boynton Beach, FL 33426.

2. On information and belief based on Apple's pleading in Paragraph 8 of its Complaint, Apple is a California corporation with its principal place of business at One Apple Park Way, Cupertino, California 95014.

JURISDICTION & VENUE

3. This Court has original jurisdiction for Corellium's counterclaims under 28 U.S.C. § 1332(a) on the grounds of diversity of citizenship. Apple is a citizen of California and Corellium is a citizen of Florida and Delaware. The amount in controversy for these claims exceeds the sum or value of $75,000.00, exclusive of costs and interest. Supplemental Jurisdiction under 28 U.S.C. § 1367 provides a further jurisdictional basis for Corellium's counterclaims.

4. Venue is proper because Apple consented to venue in this District by filing its Complaint and Demand for Jury Trial in this Court.

NATURE OF THE COUNTERCLAIMS

5. Since 2016, Apple's bug bounty program has offered external security researchers cash rewards for finding critical security vulnerabilities, i.e. bugs, in Apple's iOS. When the program was first launched in 2016, Apple offered a reward of up to $200,000 for submitting a critical vulnerability. Apple recently increased that maximum to $1,000,000.[11]

6. In order for a security researcher to receive payment for a submitted bug, the bug must be: (1) present in the most recent version of iOS; (2) accompanied by a proof of concept; and (3) the first external report of the bug.

7. Under the original 2016 bug bounty program, Apple would pay up to: (1) $200,000 for bugs in secure boot firmware components; (2) $100,000 for extraction of confidential material protected by the Secure Enclave Processor; (3) $50,000 for the execution of arbitrary code with kernel privileges; (4) $50,000 for unauthorized access to iCloud account data on Apple servers; and (5) $25,000 for access from a sandbox process to user data outside of that sandbox.

8. On August 8, 2019, just one week before filing this lawsuit, Apple announced that it would increase the size of the bug bounty reward from the prior maximum of $200,000 per vulnerability to $1,000,000 per vulnerability. Apple also announced that it would open the program to all security researchers.[12] Under the prior program, a security researcher had to be invited by Apple to participate.[13]

---

[11] David Gilbert, *Apple Will Give You $1 Million to Hack an iPhone*, VICE NEWS (Aug. 9, 2019), https://www.vice.com/en_us/article/ne8w3x/apple-will-give-you-dollar1-million-to-hack-an-iphone.

[12] Zach Whittaker, *Apple expands its bug bounty, increases maximum payout to $1M*, TECHCRUNCH (Aug. 8, 2019), https://techcrunch.com/2019/08/08/apple-hackers-macos-security/; Gilbert, *supra* note 5.

[13] Gilbert, *supra* note 11.

9. Apple invited Corellium co-founder, Chris Wade, to join its bug bounty program in April 2017. Mr. Wade has been a contributing member of the program ever since, and had contributed bugs to Apple before being invited to join the program.

10. In September 2017, Mr. Wade notified Jason Shirk at Apple that he was submitting new bugs to Apple on behalf of his new startup, Corellium, in order to fund the company. At that time, Mr. Shirk and Mr. Wade agreed to create a new developer account for Corellium so that the company could be paid directly for its submissions.

11. Apple has not paid Corellium for bugs it submitted through the bug bounty program. Specifically, Corellium has submitted the following bugs:

a. persona race condition – November 13, 2017;

b. posix_spawn issue – November 13, 2017;

c. nfssvc issue – November 13, 2017;

d. BPF race condition – January 23, 2018;

e. backboardd bug – January 23, 2018;

f. kernel execution bug – September 30, 2019; and

g. memory leak bug – September 30, 2019.

12. Apple benefited from Corellium's submission of these bugs. For example, the posix_spawn issue was addressed with iOS 11.2.5, macOS High Sierra 10.13.3, Security Update 2018-001 Sierra, Security Update 2018-001 El Capitan, tvOS 11.2.5, and watchOS 4.2.2. The nfssvc issue was addressed with macOS High Sierra 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan. Also, Apple made improvements to macOS High Sierra 10.13.4, iOS 11.3, tvOS 11.3, and watchOS 4.3 to address the persona race condition issue.

13. Despite receiving the benefit of Corellium's submissions, Apple never paid Corellium for these bugs. Under the guidelines of Apple's bug bounty program, the total value of these bugs exceeds $300,000.

14. Now, as part of its discovery in this lawsuit, Apple is requesting that Corellium disclose any and all bugs it is aware of *for free*. Apple's First Set of Requests for Production requests Corellium to provide Apple with "any bugs, exploits, vulnerabilities, or other software flaws in iOS of which Corellium or its employees currently ***are, or have ever been, aware*** (emphasis added). Through this lawsuit, Apple continues its practice of obtaining and retaining the benefit of Corellium's technology while refusing to pay for that benefit.

COUNT I: UNJUST ENRICHMENT/QUANTUM MERUIT

15. Corellium re-alleges and incorporates by reference each of the foregoing paragraphs 1-14 as if fully set forth herein.

16. Corellium's co-founder, Chris Wade, was invited to join and did join Apple's bug bounty program in April 2017.

17. In September 2017, Mr. Wade notified Mr. Shirk at Apple that he was submitting new bugs to Apple on behalf of his new startup, Corellium, in order to fund the company. At that time, Mr. Shirk and Mr. Wade agreed to create a new developer account for Corellium so that the company could be paid directly for its submissions. Soon thereafter, Mr. Wade began submitting bugs to Apple through Corellium's account.

18. Corellium submitted no fewer than seven bugs to Apple since November 2017.

19. Apple employees, including Jason Shirk, had knowledge of Corellium's participation in the bug bounty program and its submission of bugs.

20. Corellium has submitted the following bugs:

a. persona race condition – November 13, 2017;

b. posix_spawn issue – November 13, 2017;

c. nfssvc issue – November 13, 2017;

d. BPF race condition – January 23, 2018;

e. backboardd bug – January 23, 2018;

f. kernel execution bug – September 30, 2019; and

g. memory leak bug – September 30, 2019.

21. Apple benefited from Corellium's submission of these bugs. For example, the posix_spawn issue was addressed with iOS 11.2.5, macOS High Sierra 10.13.3, Security Update 2018-001 Sierra, Security Update 2018-001 El Capitan, tvOS 11.2.5, and watchOS 4.2.2. The nfssvc issue was addressed with macOS High Sierra 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan. Also, Apple made improvements to macOS High Sierra 10.13.4, iOS 11.3, tvOS 11.3, and watchOS 4.3 to address the persona race condition issue.

22. However, Apple has not paid Corellium for bugs it submitted through the bug bounty program.

23. The benefit conferred to Apple was substantial. Under the guidelines of Apple's bug bounty program, the total value of these bugs exceeds $300,000.

24. It would be inequitable for Apple to retain this benefit without paying Corellium in return.

25. Corellium requests that the Court award Corellium restitution in the amount of no less than $300,000, Corellium's court costs and pre-judgment interest from November 13, 2017, until judgment is rendered.

COUNT II: UNLAWFUL/UNFAIR BUSINESS PRACTICE

Violation of Cal. Bus. & Prof. Code § 17200, *et seq.*

26. Corellium re-alleges and incorporates by reference each of the foregoing paragraphs 1-25 as if fully set forth herein.

27. Apple invited Corellium co-founder, Chris Wade, to join its bug bounty program in April 2017. Mr. Wade has been a contributing member of the program ever since, and had contributed bugs to Apple before being invited to the program.

28. In September 2017, Mr. Wade notified Mr. Shirk at Apple that he was submitting new bugs to Apple on behalf of his new startup, Corellium, in order to fund the company. At that time, Mr. Shirk and Mr. Wade agreed to create a new developer account for Corellium so that the company could be paid directly for its submissions.

29. Apple has not paid Corellium for bugs it submitted through the bug bounty program. Specifically, Corellium has submitted the following bugs:

a. persona race condition – November 13, 2017;

b. posix_spawn issue – November 13, 2017;

c. nfssvc issue – November 13, 2017;

d. BPF race condition – January 23, 2018;

e. backboardd bug – January 23, 2018;

f. kernel execution bug – September 30, 2019; and

g. memory leak bug – September 30, 2019.

30. Apple benefited from Corellium's submission of these bugs. For example, the posix_spawn issue was addressed with iOS 11.2.5, macOS High Sierra 10.13.3, Security Update 2018-001 Sierra, Security Update 2018-001 El Capitan, tvOS 11.2.5, and watchOS 4.2.2. The

nfssvc issue was addressed with macOS High Sierra 10.13.3, Security Update 2018-001 Sierra, and Security Update 2018-001 El Capitan. Also, Apple made improvements to macOS High Sierra 10.13.4, iOS 11.3, tvOS 11.3, and watchOS 4.3 to address the persona race condition issue.

31. As alleged in Count I above, Apple was unjustly enriched by retaining the information submitted by Corellium without payment. Unjust enrichment is a predicate offense for unlawful business practices under California law. Therefore, Apple's failure to pay Corellium for bugs submitted to Apple through Apple's bug bounty program constitutes an unlawful business practice under California Business and Professions Code § 17200, *et seq*.

32. Apple is a resident of California, and at all times Apple's unlawful conduct occurred while located in California.

33. As a direct result of Apple's actions, Corellium is entitled to restitution pursuant to California Business and Professions Code § 17203 in an amount to be proved at trial.

PRAYER FOR RELIEF

Corellium, reserving its right to amend its pleadings to add additional defenses, affirmative defenses, and counterclaims if warranted by discovery, prays for the following relief:

1. A judgment in favor of Corellium on its Counterclaims and against Apple on its Complaint;

2. A judgment that Apple's Complaint be dismissed with prejudice and that Apple take nothing;

3. A judgment ordering restitution for Apple's unjust enrichment / quantum meruit and violations of California Business & Professions Code §17200, *et seq.*; and

4. Such other equitable relief, including disgorgement of all unlawfully obtained profits, that the Court finds just and proper to address and to prevent recurrence of Apple's unlawful conduct.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule 38, Corellium hereby demands trial by jury on all issues so triable raised herein, including Corellium's Counterclaims against Apple.

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on October 28, 2019, a true and correct copy of the foregoing has been transmitted by electronic filing with the Clerk of the court via CM/ECF, which will send notice of electronic filing to all counsel of record.

NORTON ROSE FULBRIGHT US LLP
Counsel for Defendant Corellium
2200 Ross Ave., Suite 3600
Dallas, Texas 75201
Telephone (214) 855-8000
Facsimile (214) 855-8200
Brett Govett, *Pro hac vice*
E-mail: brett.govett@nortonrosefulbright.com
Robert Greeson, *Pro hac vice*
E-mail: robert.greeson@ nortonrosefulbright.com
Jackie Baker, *Pro hac vice*
E-mail: jackie.baker@nortonrosefulbright.com

COLE, SCOTT & KISSANE, P.A.
Counsel for Defendant Corellium
Esperante Building
222 Lakeview Avenue, Suite 120
West Palm Beach, Florida 33401
Telephone (561) 383-9222
Facsimile (561) 683-8977
E-mail: jonathan.vine@csklegal.com
E-mail: justin.levine@csklegal.com
E-mail: lizza.constantine@csklegal.com

By:

s/ *Justin Levine*

JONATHAN VINE
Florida Bar No.: 10966
JUSTIN LEVINE
Florida Bar No.: 106463
LIZZA CONSTANTINE
Florida Bar No.: 1002945