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 TO APPLE'S FIRST AMENDED COMPLAINT

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") First Amended Complaint and Demand for Jury Trial.

RELEVANT BACKGROUND

Long before Apple accused Corellium of copyright infringement and violations of the Digital Millennium Copyright Act ("DMCA"), Apple not only encouraged Corellium to continue developing its technology, but went to great lengths to acquire Corellium and its technology. During this time, Apple approved of Corellium participating in its invitation-only Security Bounty Program ("bug bounty program") with an assurance that Apple would pay for software bugs identified by Corellium. While Apple gladly accepted and utilized bugs submitted by Corellium as part of this program, it failed to pay for them. Finally, only after the parties could not agree on an acquisition purchase price, Apple announced its own competing product and soon after sued Corellium. Tellingly, despite its lengthy discussions with Corellium's founders and familiarity with Corellium's technology, including unrestricted access to Corellium's proprietary information, Apple never hinted that it believed Corellium was infringing its copyrights or violating the DMCA.

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.

The Copyright Act is grounded in the constitutional directive to grant limited protections to the authors of copyrighted material while preserving – not suffocating – innovation. U.S. Const. art. I, § 8, cl. 8. The DMCA is no different. Congress enacted the DMCA for the purpose of preventing *digital piracy*, not to prevent innovators like Corellium from developing cutting-edge tools that benefit the public by empowering developers and researchers to more effectively and efficiently advance the security and stability of iOS devices, applications ("apps"), and services that play an integral part in end users' daily lives.

Corellium's technology is not a trafficking tool; nor does it enable others to pirate copyrighted works. Rather, Corellium's technology enables its users to run publicly available, unencrypted iOS files for the purpose of conducting advanced security research in an environment highly constrained by that purpose. Apple cannot claim that it effectively controls access to iOS when it makes iOS freely available to the public to download, open, view its object code, and run.[1] With respect to Apple's breach of DMCA allegations, it makes no sense to say that the DMCA's access control provisions apply to otherwise-readily-accessible copyrighted works. Further, use of Corellium's technology fits within the DMCA's exemptions.

In short, this lawsuit is not driven by Apple's genuine belief that Corellium infringes its copyrights or traffics a product in violation of the DMCA, but by Apple's frustration at not being able to make Corellium's technology its own and exclusively control iOS-related security research. 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 and finds no support in the letter or spirit of federal copyright law.

<u>Corellium's Innovative And Transformative Technology Has Transformed Security Research</u>

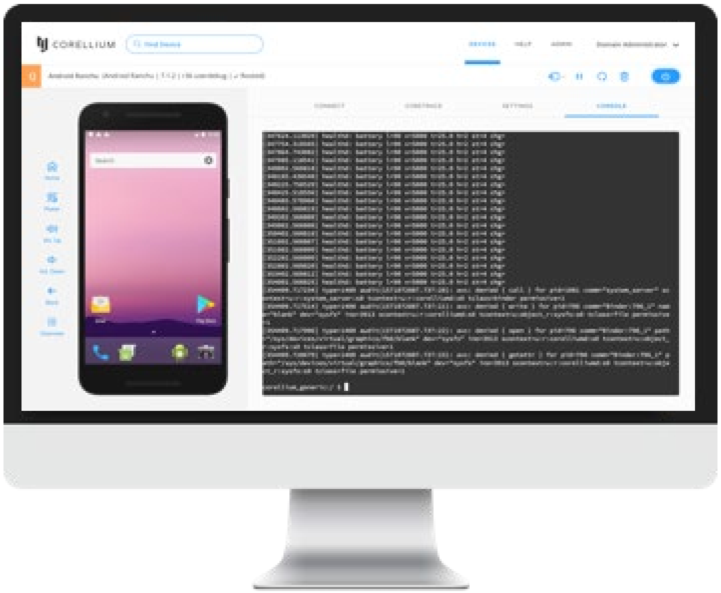
Apple wanted to purchase Corellium's technology because it is innovative and highly transformative. It virtualizes physical devices, including Apple mobile devices, enabling users to execute various device operating systems in a simple unified environment. By replacing racks of physical devices[2] with a single virtual platform, Corellium empowers software engineers to test, teach, research, and develop more efficiently and more effectively.

[1] Any person can download the iOS files, or "IPSWs," directly from Apple's servers. Direct download links can be found at https://itunes.com/versions, as well as from various third party sites including, for example, https://ipsw.me, https://www.ipswdownloader.com, and https://www.theiphonewiki.com.

[2] *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 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 having to 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 . . . ." [3]
>
> "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."[4]
>
> "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

[3] 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).

[4] 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).

> the downgrading of devices, to test fixes/bugs/features on older versions, is amazing. Then, ability to change Device IDs on the fly, with Coretrace, this is heaven."[5]

At bottom, Corellium's technology is innovative and transformative, which is why, after not being able to purchase the technology at the price it wanted, 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. Apple has credited both

[5] 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).

Corellium and Corellium users with identifying vulnerabilities in iOS that have led to significant repairs in Apple's iOS code.[6]

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 only transformed to enable it to run on different hardware, but it is also integrated with Corellium's proprietary research tool, CoreTrace, as well as several third-party tools to improve the utility of the platform for developers and researchers. Apple cannot dispute that Corellium implements its own original code, virtual machine, and proprietary research tool 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. This, of course, further illuminates Apple's motivation behind trying to make Corellium's technology its own.

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.

[6] *About the security content of iOS 13.3 and iPadOS 13.3*, APPLE.COM (Dec. 10, 2019), https://support.apple.com/en-us/HT210785 (acknowledging Corellium for informing Apple of a vulnerability which allowed "[a]n application . . . [to] be able to execute arbitrary code with kernel privileges" and noting that the "information disclosure issue was addressed by removing the vulnerable code"); *About the security content of iOS 12.4.1*, APPLE.COM (Sept. 17, 2019), https://support.apple.com/en-us/HT210549 (acknowledging Corellium user, @PWN20wnd, for their assistance in improving the security of iOS' Kernel).

Perhaps recognizing the futility of its claims for copyright infringement in light of Corellium's highly transformative nature, Apple now accuses Corellium of violating the anti-trafficking provisions of the DMCA. But the DMCA was not intended to and should not curtail activities like those promoted by Corellium's technology.[7] Consistent with the foregoing, use of Corellium's technology fits squarely within the express exemptions of the DMCA. This, of course, illustrates the fact that use of tools like those provided by Corellium are promoted – not prohibited – under the DMCA.

This is not a case of digital piracy. Corellium's technology is not a tool that enables users to bypass access controls or copy controls in iOS. Rather, Corellium's technology enables developers and researchers to run freely available, unencrypted iOS files in a new, virtual environment. As any developer or security researcher knows, Apple makes its allegedly copyrighted work – its iOS object code – available for download for free.[8] Moreover, Apple has intentionally left entire portions of its iOS code unencrypted (including the core of its operating system – the kernel) since at least 2016, well before Corellium was founded.[9] Corellium does not enable use of any iOS encrypted iOS files, nor does it facilitate decryption. By making unencrypted iOS files readily available for download for free, Apple purposefully holds the door open for developers and security researchers to help it create a better product, and to create better

[7] H.R. Rep. 105-551, pt. 2, at 38 (1998) ("The Committee believes it is very important to emphasize that Section 102(a)(2) [now codified as 17 U.S.C. § 1201(a)(2)] is aimed fundamentally at outlawing so-called 'black boxes' that are expressly intended to facilitate circumvention of technological protection measures for purposes of gaining access to a work. This provision is not aimed at products that are capable of commercially significant noninfringing uses, such as consumer electronics, telecommunications, and computer products—including videocassette recorders, telecommunications switches, personal computers, and servers--used by businesses and consumers for perfectly legitimate purposes."); *Id.* at 40 (stating the same intent with respect to Section 102(b)(1), now codified under 17 U.S.C. § 1201(b)).

[8] *See supra*, note 1.

[9] Kate Conger, *Apple confirms iOS kernel code left unencrypted intentionally*, TECHCRUNCH (June 22, 2016), https://techcrunch.com/2016/06/22/apple-unencrypted-kernel/.

products of their own. Corellium simply enables developers and security researchers to do this in a more productive way.

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 and acquire their innovative technology 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.[10] 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 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 nearly identical to the technology offered by Corellium. Within six months, Mr. Wade, Ms. Gorton, and Mr. Skowronek were asked by Apple to enter into a letter of intent with the company for the acquisition of Virtual. The team decided to sell their company to Fort Lauderdale-based Citrix instead.

[10] *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.

Apple's Subsequent Attempts To Purchase Corellium

Apple's interest in Corellium's founders and their innovative technology did not end with Virtual. In January 2018, Apple entered into negotiations with Mr. Wade and Ms. Gorton to purchase Corellium. The two companies entered into a Confidentiality Agreement for Possible Transaction (the "Non-Disclosure Agreement") on January 25, 2018, after which Corellium provided Apple access to its platform and technical information concerning its underlying functionality.

In the six months that followed, Corellium's founders travelled to Cupertino, California at least three times to meet with Apple executives, including Apple's Vice President of Software Engineering, Jon Andrews, and Apple's Senior Vice President of Software Engineering, Craig Federighi, about a potential acquisition. While doing so, Corellium shared detailed technical information with Apple and demonstrated its technology to Apple's security and software engineering teams several times. Corellium also participated in a full-day technical review of its platform conducted by Apple in March 2018. In June 2018, Corellium provided Mr. Andrews with a Corellium user account along with access to Corellium's APIs.

During Apple and Corellium's negotiations, Apple never indicated to Corellium's founders that it believed Corellium was infringing its copyrights or violating the DMCA. Nor did Apple send Corellium or its founders any cease and desist letter. Instead, Apple encouraged Corellium's founders to "come demo" their product in Cupertino and suggested that Apple had a "good idea of how [Corellium's] team could have a big impact and build on the core technology." Then, nearly a year and a half after Apple began exploring a possible acquisition of Corellium, Apple – without warning – filed this lawsuit.

Apple's Use Of Corellium's Technology

In the months leading up to Apple's negotiations with Corellium, Apple 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: why pay for bugs when you are going to own the company submitting the bugs?

Due to Apple's refusal to pay, it is Apple that owes Corellium. Rather than paying Corellium, Apple is now trying to receive 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.

After Failing To Acquire Corellium, 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.[11]

[11] Lorenzo Francecshi-Bicchierai, *Apple's Lawsuit Against a Startup Shows How It Wants to Control the iPhone Hacking Market*, VICE NEWS (Aug. 16, 2019), https://www.vice.com/en_us/article/d3a8jq/apple-corellium-lawsuit.

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. 56, ¶ 43. 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? Because it was not able to purchase Corellium or its predecessor company, Virtual, for the price it wanted. Consequently, Apple did the only thing it knew to do when it could not acquire Corellium for less than fair market value – file a lawsuit accusing Corellium of copyright infringement and DMCA violations – even though Apple was not only aware of Corellium's technology for several years, but actually encouraged its development.

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.[12] It also infected the phones of non-Uyghurs and forced the FBI to ask Google to de-index the offending websites in order to reduce the number of infections.[13]

[12] Zach Whittaker, *Sources Say China Used iPhone Hacks to Target Uyghur Muslims*, TECHCRUNCH (Aug. 31, 2019), https://techcrunch.com/2019/08/31/china-google-iphone-uyghur/.

[13] 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/.

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.[14] 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.[15]

Corellium agrees. Corellium's technology is intended to improve the security research and development community. Apple's copyrights and the DMCA 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 FIRST AMENDED COMPLAINT

1. Corellium admits 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.

4. Denied.

5. Denied.

6. Denied.

7. Denied.

[14] 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.

[15] Lakshmanan, *supra* note 13.

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.

23. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 23, and therefore denies same.

24. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 24, and therefore denies same.

B. Corellium’s Infringing Product

25. Denied.

26. Denied.

27. Denied.

28. Denied.

29. Denied.

30. Denied.

31. Denied.

32. Denied.

33. Denied.

34. Denied.

35. Denied.

36. Corellium admits that the statements referenced in paragraph 36 purport to be attributable to Mr. Wade. The statements speak for themselves, and Corellium denies the allegations contained in paragraph 36 to the extent Apple attempts to characterize same.

37. Corellium admits that Mr. Wade appeared on a podcast called Risky Business. Corellium admits that the statements referenced in paragraph 37 purport to be attributable to Mr. Wade. The statements speak for themselves, and Corellium denies the allegations contained in paragraph 37 to the extent Apple attempts to characterize same.

38. Denied.

39. Denied.

40. Denied.

41. Corellium denies the allegations contained in paragraph 41, except that Corellium admits that Corellium and its founders do business with those working in software security to protect end users.

42. Denied.

43. Corellium admits that the statements referenced in paragraph 43 purport to be attributable to Mr. Wade. The statements speak for themselves, and Corellium denies the allegations contained in paragraph 43 to the extent Apple attempts to characterize same.

44. Denied.

C. Corellium's Acts of Copyright Infringment

45. Denied.

46. Denied.

47. Denied.

D. Corellium's Unlawful Trafficking of a Product Used To Circumvent Security Measures

48. Paragraph 48 contains legal conclusions to which no answer is required. To the extent an answer is necessary, Corellium denies the allegations contained in paragraph 48.

49. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 49, and therefore denies same.

50. Denied.

FIRST CLAIM FOR RELIEF

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

51. Corellium realleges and incorporates by reference each of the answers and responses in preceding paragraphs 1-50 set forth above.

52. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 52, and therefore denies same.

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. Denied.

55. Denied.

56. Denied.

57. Denied.

SECOND CLAIM FOR RELIEF

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

58. Corellium realleges and incorporates by reference each of the answers and responses in preceding paragraphs 1-50 set forth above.

59. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 59, and therefore denies same.

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.

THIRD CLAIM FOR RELIEF

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

65. Corellium realleges and incorporates by reference each of the answers and responses in preceding paragraphs 1-50 set forth above.

66. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 66, and therefore denies same.

67. Denied.

68. Denied.

69. Denied.

70. Denied.

FOURTH CLAIM FOR RELIEF

Unlawful Trafficking, 17 U.S.C. § 1201(a)(2), (b), 1203

71. Corellium realleges and incorporates by reference each of the answers and responses in preceding paragraphs 1-50 set forth above.

72. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 72, and therefore denies same.

73. Corellium lacks knowledge or information sufficient to form a belief as to the truth of the allegations contained in paragraph 73, and therefore denies same.

74. Denied.

75. Denied.

76. Denied.

77. 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 because they consist 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.

SIXTEENTH AFFIRMATIVE DEFENSE
(Failure to State a Claim – No Copyright Infringement)

16. For its sixteenth affirmative defense, Corellium states that Plaintiff fails to state a claim under the Digital Millennium Copyright Act because Corellium has not infringed Apple's alleged copyrighted works. As such, there can be no nexus between any possible infringement and the use of any alleged circumvention device.

SEVENTEENTH AFFIRMATIVE DEFENSE
(Constitutionality of 17 U.S.C. §§ 1201(a)(2) & (b))

17. For its seventeenth affirmative defense, Corellium states that the asserted provisions of the Digital Millennium Copyright Act upon which Apple sues violate the First Amendment to the United States Constitution.

EIGHTEENTH AFFIRMATIVE DEFENSE
(17 U.S.C. § 1201(c)(4) – Free Speech)

18. For its eighteenth affirmative defense, Corellium states that Apple's Digital Millennium Copyright Act claims against Corellium are prohibited under 17 U.S.C. § 1201(c)(4) because enforcement of such claims impermissibly diminishes Corellium's right of free speech in its use of consumer electronics, telecommunications, and/or computing products.

NINTEENTH AFFIRMATIVE DEFENSE
(No Circumvention Enabled)

19. For its ninteenth affirmative defense, Corellium states that Plaintiff fails to state a cause of action under the Digital Millennium Copyright Act because Corellium does not traffic

any technology, product, service, device, component, or part thereof, that enables Corellium's users to circumvent a technological measure that effectively controls access to a work protected under the Copyright Act.

TWENTIETH AFFIRMATIVE DEFENSE
(17 U.S.C. § 1201(c)(1) – Fair Use)

20. For its twentieth affirmative defense, Corellium states that Apple's Digital Millennium Copyright Act claims against Corellium are prohibited under 17 U.S.C. § 1201(c)(1) because Corellium makes fair use of Apple's allegedly copyrighted works.

TWENTY-FIRST AFFIRMATIVE DEFENSE
(17 U.S.C. § 1201(f) – Reverse Engineering)

21. For its twenty-first affirmative defense, Corellium states that to the extent the Court determines that Corellium's technology enables circumvention of a technological measure or protection afforded by a technological measure, Corellium is exempted from liability under the Digital Millennium Copyright Act by subsection 1201(f) of the Digital Millennium Copyright Act as Corellium's technology enables identification and analysis of elements of a computer program necessary to achieve interoperability of an independently created computer program with other programs and/or makes such means available to others for the purpose of enabling interoperability of an independently created computer program with other programs.

TWENTY-SECOND AFFIRMATIVE DEFENSE
(17 U.S.C. § 1201(g) – Encryption Research)

22. For its twenty-second affirmative defense, Corellium states that to the extent the Court determines that Corellium's technology enables circumvention of a technological measure, Corellium is exempted from liability under the Digital Millennium Copyright Act by subsection 1201(g) of the Digital Millennium Copyright Act as Corellium's technology was

developed to perform good faith encryption research and is provided to its users for the purpose of conducting acts of good faith encryption research.

TWENTY-THIRD AFFIRMATIVE DEFENSE (17 U.S.C. § 1201(j) – Security Testing)

23. For its twenty-third affirmative defense, Corellium states that it is exempted from liability under the Digital Millennium Copyright Act by subsection 1201(j) of the Digital Millennium Copyright Act because Corellium developed, produced, and/or employed technological means solely for the purpose of performing acts of security testing.

TWENTY-FOURTH AFFIRMATIVE DEFENSE (37 C.F.R. § 201.40(b)(6) – Jailbreaking)

24. For its twenty-fourth affirmative defense, Corellium states that it is exempted from liability under the Digital Millennium Copyright Act by 37 C.F.R. § 201.40(b)(6) because Corellium facilitates noninfringing uses of computer programs that enable smartphones and portable all-purpose mobile computing devices to execute lawfully obtained software applications, where circumvention is accomplished for the sole purpose of enabling interoperability of such applications with computer programs on the smartphone or device, or to permit removal of software from the smartphone or device.

TWENTY-FIFTH AFFIRMATIVE DEFENSE (37 C.F.R. § 201.40(b)(11) – Good Faith Security Research)

25. For its twenty-fifth affirmative defense, Corellium states that it is exempted from liability under the Digital Millennium Copyright Act by 37 C.F.R. § 201.40(b)(11) because Corellium facilitates noninfringing uses of computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates, or is undertaken on a computer, computer system, or computer network on which the computer

program operates with the authorization of the owner or operator of such computer, computer system, or computer network, solely for the purpose of good-faith security research.

26. 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 Federal Rule of Civil Procedure 8, as they may become known through the discovery process

COUNTERCLAIMS AGAINST APPLE

Corellium brings the following Counterclaims against 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, Florida 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. Apple wants to limit and control, not expand, security research.

6. Apple has long been said to have a "rough relationship with [security] researchers."[16] In the fall of 2016, likely to combat this perceived hostility to security research, Apple announced its bug bounty program, which for the first time offered external security researchers cash rewards for finding critical security vulnerabilities, i.e., bugs, in Apple's iOS. Apple's announcement was hailed as a "step in the right direction" by the security research community.[17]

7. But since that first announcement, it has become clear that Apple is unfairly withholding payments for submissions that otherwise satisfy the bug bounty program.

8. Moreover, Apple's bug bounty program serves as an example of the company's attempts to curry favor with the security research community, while internally working to limit and control security research. On information and belief, Apple has created this program as an effort to induce submissions that Apple has no intent to pay for.

Apple's Control Over The Bug Bounty Program

9. Apple's bug bounty program policy is: "Heads I win, tails you lose."

10. The program is governed by a policy titled: "Apple Security Bounty Program Policy." The policy is a proposed course of action—not a contract or agreement.

[16] Kate Conger, *Apple Announces Long-Awaited Bug Bounty Program*, TECHCRUNCH (Aug. 4, 2016), https://techcrunch.com/2016/08/04/apple-announces-long-awaited-bug-bounty-program/.

[17] *Id.*

11. The intent of the bug bounty program is to induce security researchers to act for the benefit of Apple. In Apple's own words, the program "is going to reward researchers who actually share critical vulnerabilities with Apple."[18]

12. Apple actively encourages security researchers to participate in its bug bounty program by offering rewards for bugs that qualify under the Security Bounty Program Policy.

13. In the Security Bounty Program Policy, Apple promises it "will pay cash rewards for security vulnerabilities found in specific Apple services and products, to researchers who abide by the guidelines" of the program.

14. At the same time, "[p]ayments are at Apple's sole discretion", "[r]ewards are granted solely at the exclusive discretion of Apple", "[t]he terms, program scope, and payments are all subject to change at Apple's sole discretion", and "[t]he program may be terminated at any time."

15. Through the Security Bounty Program Policy, Apple retains sole and complete discretion to determine whether to pay a participant for a submission, even if the submission meets or exceeds Apple's guidelines. For instance, under the policy, a participant could provide Apple with a bug that clearly conforms with the policy, but Apple could decline to pay the participant for that submission.

16. What's more, a participant in Apple's bug bounty program is "ask[ed]" to keep his or her "involvement with the program confidential." And before disclosing any information about an issue reported under the bug bounty program to other parties, a participant is also required to let Apple:

[18] Ivan Krstić, *Behind The Scenes With iOS Security*, Address at Black Hat USA 2016 Conference, YOUTUBE.COM (Aug. 16, 2016), https://www.youtube.com/watch?v=BLGFriOKz6U.

a. validate the report;

b. diagnose the vulnerability;

c. implement a fix or other corrective measure;

d. validate the fix against all affected platforms; and

e. distribute the fix to its customers.

17. In that same vein, under Apple's Security Bounty Program Policy, Apple asks that participants share any public comments about the reported bug with Apple first before releasing those comments publicly.

The Bug Bounty Program

18. When first announced in 2016, Apple's bug bounty program offered a reward of up to $200,000 for submitting a critical vulnerability. Apple recently increased that maximum to $1,000,000.[19]

19. 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.

20. 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.

[19] 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.

21. On August 8, 2019, just one week before filing this lawsuit, Apple announced that it would increase the amount 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.[20]

22. Under the earlier bug bounty program, a security researcher had to be invited by Apple to participate in the program.[21] However, any security researcher outside the program could still submit a bug to Apple in the hopes of being invited to join the program and receive payment.[22]

23. On August 8, 2019, Apple simultaneously announced that it will provide new dev devices for use in conjunction with its bug bounty program to security researchers on an invite-only basis.[23] Apple touted these devices as an "Apple-supported iOS security research platform" targeted to security researchers "who have been focused on other platforms."[24] On information and belief, these devices will likely be subject to strict nondisclosure agreements, further revealing Apple's intent to control and limit, not expand, security research.

24. Apple's announcement, just days before bringing this lawsuit, has been viewed by some as "part of the same strategy" of "attempting to control what security researchers do with iPhones."[25]

[20] 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 19.

[21] Gilbert, *supra* note 19.

[22] Krstić, *supra* note 18.

[23] Ivan Krstić, *Behind The Scenes Of iOS And Mac Security*, Address at Black Hat USA 2019 Conference (Aug. 2019), https://i.blackhat.com/USA-19/Thursday/us-19-Krstic-Behind-The-Scenes-Of-IOS-And-Mas-Security.pdf.

[24] *Id.*

[25] Franceschi-Bicchierai, *supra* note 11.

Corellium's Participation In Apple's Bug Bounty Program

25. 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.

26. 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 that Corellium could be paid directly for its submissions.

27. 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.

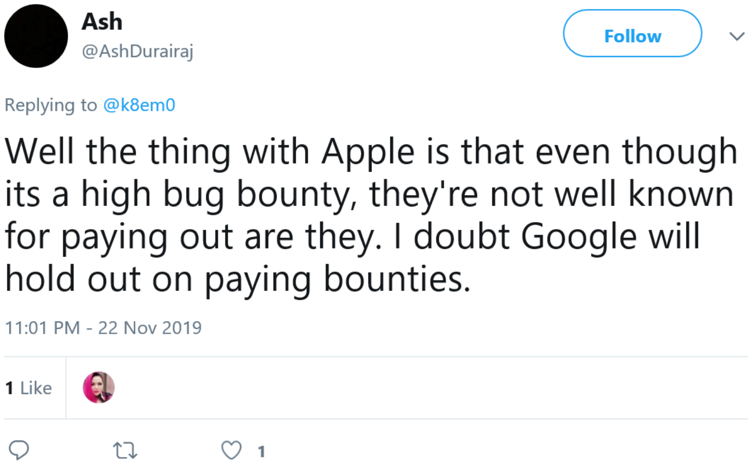
28. Apple benefited from Corellium's submission of these bugs. For example, the posix_spawn issue was addressed with iOS 11.2.5, macOS High Sierra 10.13.3, Security Update 2018-001 Sierra, Security Update 2018-001 El Capitan, tvOS 11.2.5, and watchOS 4.2.2. The nfssvc issue was addressed with macOS High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

29. 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 market value of these bugs is, at a minimum, $300,000.

30. 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.

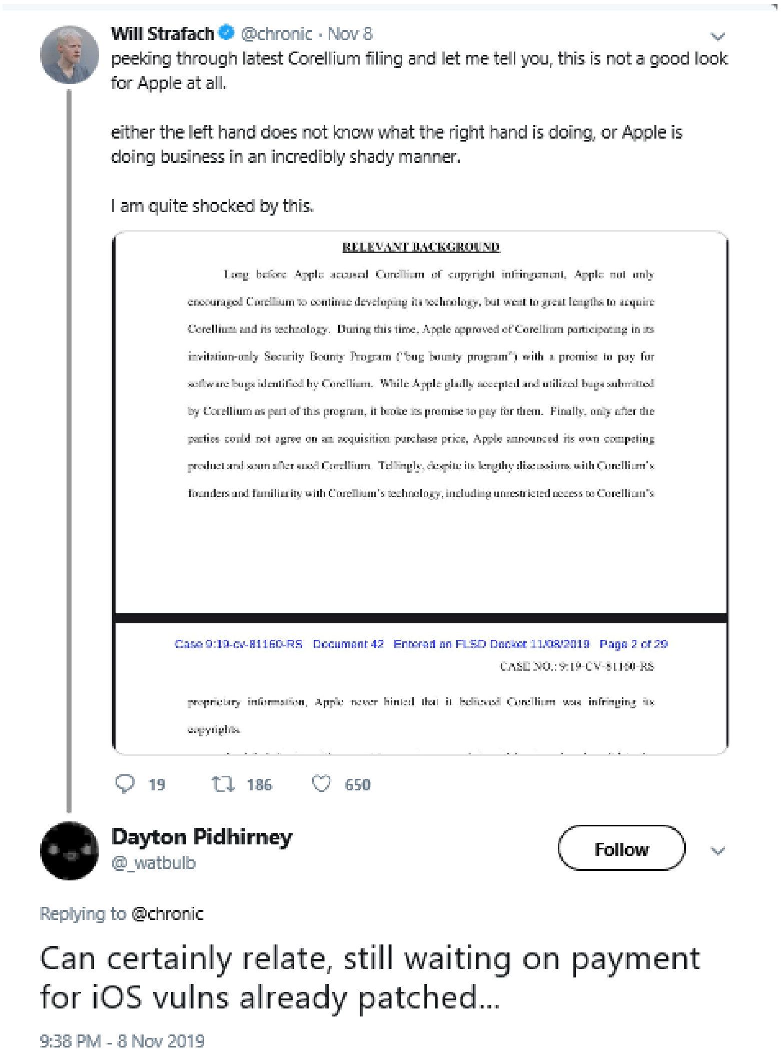
<u>Apple's Pattern And Practice Of Controlling The Security Research Industry</u>

31. Through this pattern and practice, Apple has garnered a reputation for failing to pay security researchers for their bug bounty submissions:



Well the thing with Apple is that even though its a high bug bounty, they're not well known for paying out are they. I doubt Google will hold out on paying bounties.

32. Apple has not paid many participants of its invite-only program. One bug bounty program member writes that he is still waiting for payment from Apple for iPhone vulnerabilities:



Will Strafach @chronic · Nov 8

peeking through latest Corellium filing and let me tell you, this is not a good look for Apple at all.

either the left hand does not know what the right hand is doing, or Apple is doing business in an incredibly shady manner.

I am quite shocked by this.

RELEVANT BACKGROUND

Long before Apple accused Corellium of copyright infringement, Apple not only encouraged Corellium to continue developing its technology, but went to great lengths to acquire Corellium and its technology. 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, only after the parties could not agree on an acquisition purchase price, Apple announced its own competing product and soon after sued Corellium. Tellingly, despite its lengthy discussions with Corellium's founders and familiarity with Corellium's technology, including unrestricted access to Corellium's

Case 9:19-cv-81160-RS Document 42 Entered on FLSD Docket 11/08/2019 Page 2 of 29

CASE NO.: 9:19-CV-81160-RS

proprietary information, Apple never hinted that it believed Corellium was infringing its copyrights.

19 186 650

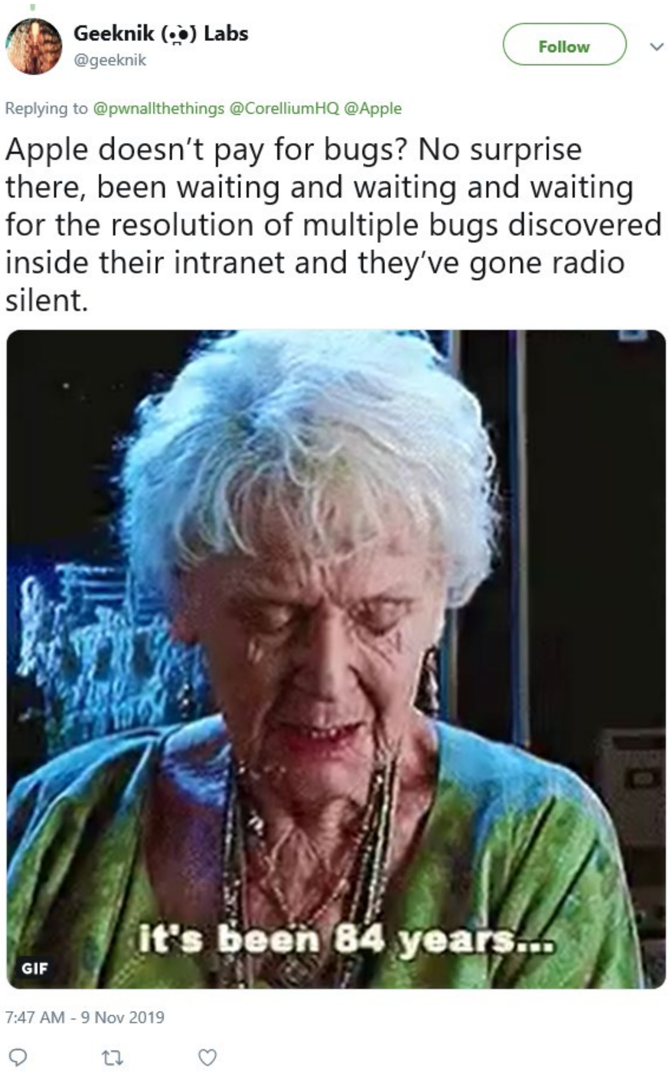
Dayton Pidhirney
@_watbulb

Replying to @chronic

Can certainly relate, still waiting on payment for iOS vulns already patched...

9:38 PM - 8 Nov 2019

33. Another bug bounty program member writes:



Geeknik (•͜•) Labs
@geeknik

Replying to @pwnallthethings @CorelliumHQ @Apple

Apple doesn't pay for bugs? No surprise there, been waiting and waiting and waiting for the resolution of multiple bugs discovered inside their intranet and they've gone radio silent.

7:47 AM - 9 Nov 2019

34. On information and belief, Apple never intended to pay bug bounty program participants for every qualifying submission.

35. Just like its potential acquistion of Corellium, Apple encourages conduct beneficial to Apple until it decides the price is too high. A familiar theme emerges from Apple's conduct in the security research field: (1) Apple encourages members of the security research community to work in confidence with Apple, the results of which benefit Apple and its products; (2) Apple incentivizes this conduct by offering monetary rewards; and (3) if Apple decides the price is too

high, it silently elects not to purchase or pay the earned bounty – or it sues the party, like it did with Corellium.

36. It is clear that Apple seeks to retain control and absolute discretion over who performs security research and how that research is performed. This is why Apple's bug bounty program policy is: "Heads I win, tails you lose."

37. Apple's conduct with respect to the bug bounty program also fails to honor, much less pay lip service, to the following lofty statement contained in the Apple Supplier Code of Conduct: "Apple expects the highest standards of ethical conduct in all of our endeavors." Unfortunately, Apple fails to practice what it preaches with respect to security researchers.[26] This pattern of behavior is consistent with other reported conduct by Apple failing to practice what it preaches with respect to its Supplier Code of Conduct.[27]

<u>COUNT I: DECLARATORY JUDGMENT</u>
28 U.S.C. § 2201

38. Corellium re-alleges and incorporates by reference paragraphs 1-37 as if fully set forth herein.

39. Apple's bug bounty program is governed by a policy titled: "Apple Security Bounty Program Policy."

40. Apple's Security Bounty Program Policy specifies that Apple has sole discretion to pay or not pay for bug bounty program participant submissions.

[26] *Apple Supplier Code of Conduct*, APPLE.COM, https://www.apple.com/supplier-responsibility/ (last visited Nov. 26, 2019).

[27] Thomas Clarke & Martijn Boersma, *Apple, The $1Trillion Company Searching For Its Soul*, THECONVERSATION.COM (Aug. 5, 2018), https://theconversation.com/apple-the-1-trillion-company-searching-for-its-soul-101030.

41. Apple's Security Bounty Program Policy also specifies that the program, the program's scope, and payments are all subject to change at Apple's sole discretion and that the program may be terminated at any time.

42. The purported consideration flowing from Apple is illusory. There is no promise to pay on the part of Apple even if the bug bounty program participant completely performs under the Security Bounty Program Policy.

43. Therefore, there is no binding or enforceable agreement pursuant to Apple's Security Bounty Program Policy.

44. As such, Corellium requests that the Court declare that Apple's Security Bounty Program Policy is not an enforceable contract or agreement on its face, that any purported consideration is illusory, and, therefore, there is no binding or enforceable agreement between Apple and Corellium pursuant to Apple's Security Bounty Program Policy.

COUNT II: DECLARATORY JUDGMENT
28 U.S.C. § 2201

45. Corellium re-alleges and incorporates by reference paragraphs 1-44 as if fully set forth herein.

46. The Security Bounty Program Policy does not mention or incorporate by reference any other agreement and no other agreement mentions or incorporates by reference the Security Bounty Program Policy.

47. As such, Corellium requests that the Court declare that there is no binding or enforceable agreement between Apple and Corellium under the Security Bounty Program Policy, any other written agreement, or any combination thereof.

COUNT III: CONSTRUCTIVE FRAUD
Cal. Civ. Code § 1573

48. Corellium re-alleges and incorporates by reference paragraphs 1-47 as if fully set forth herein.

49. This is an action against Apple for constructive fraud in violation of California Civil Code § 1573.

50. In September 2017, Corellium became a participant in Apple's bug bounty program, which placed Corellium in a confidential relationship with Apple.

51. Corellium placed its trust and confidence in Apple. Specifically, Corellium understood Apple's representation that it "will pay cash rewards for security vulnerabilities found in specific Apple services and products, to researchers who abide by the guidelines[,]" as set forth in the Security Bounty Program Policy, to mean that Corellium would be paid for submitting conforming bugs to Apple as part of the bug bounty program.

52. Further, Apple's Security Bounty Program Policy also requests that participants keep their involvement in the program confidential and that participants receive approval from Apple before commenting publicly on any submission.

53. In reliance on these representations, Corellium searched for, identified, and submitted the following bugs to Apple:

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.

54. Apple addressed Corellium's submissions in subsequent software updates. 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.

55. Apple has not paid Corellium for these bugs and, therefore, has breached its duty arising from the confidential relationship.

56. Apple has received an unfair advantage, which has prejudiced Corellium. Apple induced Corellium to submit bugs and used those submissions to correct and update its software. Apple did not pay Corellium for the benefit it conferred.

57. Under the guidelines of Apple's Security Bounty Program Policy, the total market value of these bugs is, at a minimum, $300,000.

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

59. Corellium requests that the Court award Corellium damages in the amount of no less than $300,000, Corellium's court costs, and pre-judgment interest.

COUNT IV: CONSTRUCTIVE FRAUD
Florida Common Law

60. Corellium re-alleges and incorporates by reference paragraphs 1-59 as if fully set forth herein.

61. This is an action against Apple for constructive fraud under Florida common law.

62. In September 2017, Corellium became a participant in Apple's bug bounty program, which placed Corellium in a confidential relationship with Apple.

63. Corellium placed its trust in Apple and depended on Apple to act in good faith when ajudicating any bugs Corellium submitted to Apple. Specifically, Corellium understood Apple's representation that it "will pay cash rewards for security vulnerabilities found in specific Apple services and products, to researchers who abide by the guidelines[,]" as set forth in the Security Bounty Program Policy, to mean that it would be paid for submitting conforming bugs to Apple as part of the bug bounty program.

64. Apple's Security Bounty Program Policy also requests that participants keep their involvement in the program confidential and that participants receive approval from Apple before commenting publicly on any submission.

65. In reliance on these representations, Corellium submitted the following bugs to Apple:

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.

66. Apple used Corellium's submissions to correct and update its software. 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.

67. Apple has not paid Corellium for these bugs and, therefore, has breached its duty arising from the confidential relationship.

68. Apple's actions improperly advantaged Apple at Corellium's expense because Apple received and utilized the benefit of Corellium's work without adequately compensating Corellium for that use.

69. Under the guidelines of Apple's Security Bounty Program Policy, the total market value of these bugs is, at a minimum, $300,000.

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

71. Corellium requests that the Court award Corellium damages in the amount of no less than $300,000, Corellium's court costs, and pre-judgment interest.

COUNT V: UNLAWFUL BUSINESS PRACTICE: CONSTRUCTIVE FRAUD
Violation of Cal. Bus. & Prof. Code § 17200, *et seq.*

72. Corellium re-alleges and incorporates by reference paragraphs 1-71 as if fully set forth herein.

73. This is an action against Apple for unlawful business practices in violation of California Business & Professions Code § 17200, *et seq*.

74. In September 2017, Corellium became a participant in Apple's bug bounty program, which placed Corellium in a special confidential relationship with Apple.

75. Corellium placed its trust and confidence in Apple. Specifically, Corellium understood Apple's representation that it "will pay cash rewards for security vulnerabilities found in specific Apple services and products, to researchers who abide by the guidelines[,]" as set forth in the Security Bounty Program Policy, to mean that Corellium would be paid for submitting conforming bugs to Apple as part of the bug bounty program.

76. Further, Apple's Security Bounty Program Policy requests that participants keep their involvement in the program confidential and that participants receive approval from Apple before commenting publicly on any submission.

77. In reliance on these representations, Corellium submitted the following bugs to Apple:

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.

78. Apple addressed Corellium's submissions in subsequent software updates. 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.

79. Apple has not paid Corellium for these bugs and, therefore, has breached its duty arising from the confidential relationship.

80. Apple has received an unfair advantage, which has prejudiced Corellium. Apple induced Corellium to submit bugs and used those submissions to correct and update its software. Apple did not pay Corellium for the benefit it conferred.

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

82. As a result of Apple's conduct described herein, Corellium has sustained and will continue to sustain irreparable injury for which no adequate remedy at law exists.

83. As alleged in Count III above, Apple's conduct constitutes constructive fraud under California law. Constructive fraud is a predicate offense for unlawful business practices under California Business & Professions Code § 17200, *et seq*. 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 & Professions Code § 17200, *et seq*.

84. As a direct result of Apple's actions, Corellium is entitled to restitution pursuant to California Business & Professions Code § 17203 in an amount to be proven at trial. In addition, Corellium requests that the Court permanently enjoin Apple from engaging in the unlawful and wrongful acts outlined in this Count. Finally, Corellium requests a declaration that Apple's unlawful acts outlined in this Count constitute an unlawful business practice in violation of California Business & Professions Code § 17200, *et seq*.

COUNT VI: UNFAIR BUSINESS PRACTICES
Violation of Cal. Bus. & Prof. Code § 17200, *et seq.*

85. Corellium re-alleges and incorporates by reference paragraphs 1-84 as if fully set forth herein.

86. This is an action against Apple for unfair business practices in violation of California Business & Professions Code § 17200, *et seq*.

87. Apple's administration of the bug bounty program, including, but not limited to, Apple's conduct in enticing members of the security research community to search for and identify bugs, develop exploits for those bugs, and submit bugs to Apple, despite having no intention to and not actually paying for those submissions is an unfair business practice under California law.

88. Since 2016, Apple has invited security researchers to participate in its invite-only bug bounty program.

89. Apple's bug bounty program is intended to encourage and reward security researchers for submitting qualifying bugs to Apple.

90. Apple's program encourages security researchers to search for, identify, and develop exploits for bugs in Apple's iOS by offering cash rewards to participants.

91. Once a participant performs these tasks and submits a bug to Apple that meets Apple's Security Bounty Program Policy guidelines, however, Apple does not pay for those submissions.

92. Specifically, Apple represents to its bug bounty program participants, including Corellium, that Apple will pay participants for submitting bugs to Apple that comply with the bug bounty program policy.

93. Corellium understood Apple's representation that Apple "will pay cash rewards for security vulnerabilities found in specific Apple services and products, to researchers who abide by

the guidelines[,]" as set forth in the Security Bounty Program Policy, to mean that Corellium would be paid for submitting conforming bugs to Apple pursuant to the bug bounty program.

94. Based on that representation, Corellium submitted the following bugs to Apple:

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.

95. Apple has not paid Corellium for those submissions. Apple has, however, used those submissions to correct and update its software on various occasions.

96. Corellium was injured by Apple's failure to pay Corellium for its submissions.

97. Apple has a pattern and practice of engaging in the unfair conduct specified herein. In addition to Corellium, several other security researchers have not received payment for their submission of conforming bugs to Apple through the bug bounty program.

98. On information and belief, Apple has not and does not intend to pay for every conforming bug that is submitted to its bug bounty program.

99. Apple's conduct prevents competition and controls the security research business by enticing members of the security research community to participate in and submit valuable bugs to Apple for which it has no intention of paying.

100. The Security Bounty Program Policy—including the requirement that a participant "must allow Apple the opportunity" to validate and diagnose a bug, and implement and distribute

a fix before the participant can reveal the bug to a third party—demonstrates that the program is intended to control and limit iOS security research.

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

102. As a result of Apple's conduct described herein, Corellium has sustained and will continue to sustain irreparable injury for which no adequate remedy at law exists.

103. 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. In addition, Corellium seeks that the Court permanently enjoin Apple from engaging in the unfair and anticompetitive acts outlined in this Count. Finally, Corellium requests a declaration that Apple's unfair and anticompetitive acts outlined in this Count constitute an unfair business practice in violation of California Business & Professions Code § 17200, *et seq*.

COUNT VII: DECEPTIVE AND UNFAIR TRADE PRACTICES
Violation of Fla. Stat. § 501.201, *et seq.*

104. Corellium re-alleges and incorporates by reference paragraphs 1-103 as if fully set forth herein.

105. This is an action against Apple for deceptive and unfair trade practices in violation of Florida Statute § 501.201, *et seq*.

106. Apple's administration of the bug bounty program, including, but not limited to, Apple's conduct in enticing members of the security research community to search for and identify bugs, develop exploits for those bugs, and submit bugs to Apple, despite having no intention to and not actually paying for those submissions is an unfair and/or deceptive trade practice under Florida law.

107. Since 2016, Apple has invited security researchers to participate in its invite-only bug bounty program.

108. Apple's bug bounty program is intended to encourage and reward security researchers for submitting qualifying bugs to Apple.

109. Apple's program motivates security researchers to search for, identify, and develop exploits for bugs in Apple's iOS by offering cash rewards to participants.

110. Once a participant performs these tasks and submits a bug to Apple that meets the guidelines of the Security Bounty Program Policy, however, Apple does not pay for those submissions.

111. Specifically, Apple represents to participants in its bug bounty program, including Corellium, that Apple will pay participants for submitting bugs to Apple that comply with the bug bounty program policy.

112. Corellium understood Apple's representation that Apple "will pay cash rewards for security vulnerabilities found in specific Apple services and products, to researchers who abide by the guidelines[,]" as set forth in the Security Bounty Program Policy, to mean that Corellium would be paid for submitting conforming bugs to Apple pursuant to the bug bounty program.

113. Relying on these representations, Corellium submitted the following bugs to Apple:

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.

114. Apple has not paid Corellium for these bugs. However, Apple has used these submissions to correct and update its software on various occasions.

115. Apple's conduct, as alleged herein, is a common practice. In addition to Corellium, several security researchers have not received payment for their submission of conforming bugs to Apple through the bug bounty program.

116. On information and belief, Apple has not and does not intend to pay for every conforming bug that is submitted to its bug bounty program.

117. Apple's conduct prevents competition and controls the security research business. Apple entices members of the security research community to participate in and submit valuable bugs to Apple for which it has no intention of paying. This conduct is unfair and/or deceptive.

118. The Security Bounty Program Policy—including the requirement that a participant "must allow Apple the opportunity" to validate and diagnose a bug, and implement and distribute a fix before the participant can reveal the bug to a third party—demonstrates that the program is intended to control and limit iOS security research.

119. Apple's pattern and practice of outwardly appearing to support security research, while inwardly working to stifle that research, adds additional color to Apple's conduct alleged herein.

120. As a result of Apple's conduct described herein, Corellium has sustained and will continue to sustain irreparable injury for which no adequate remedy at law exists.

121. Further, as a direct and proximate result of Apple's conduct, Corellium has been, and is being, damaged.

122. Corellium requests that the Court award Corellium actual damages resulting from the unfair and deceptive acts, Corellium's court costs, pre-judgment interest, and attorneys' fees pursuant to Fla. Stat. § 501.2105. In addition, Corellium seeks that the Court permanently enjoin Apple from engaging in the wrongful and deceptive acts outlined in this Count. Finally, Corellium requests a declaration that Apple's wrongful and deceptive acts outlined in this Count constitutes a violation of Fla. Stat. § 501.201, *et seq*.

COUNT VIII: UNJUST ENRICHMENT/QUANTUM MERUIT
Under California Common Law

123. Corellium re-alleges and incorporates by reference paragraphs 1-122 as if fully set forth herein.

124. This is an action for unjust enrichment/quantum meruit against Apple under California common law.

125. Apple's bug bounty program is described in the document: "Apple Security Bounty Program Policy." This document is a policy, a proposed course of action—not a contract or agreement.

126. In September 2017, Corellium became a participant in Apple's bug bounty program.

127. As part of that program, Corellium submitted no fewer than seven bugs to Apple since November 2017.

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

129. Corellium submitted the following bugs to Apple:

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.

130. 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.

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

132. The benefit conferred to Apple was substantial. Under the guidelines of Apple's bug bounty program, the total market value of these bugs is, at a minimum, $300,000.

133. It would be unjust for Apple to retain this benefit at Corellium's expense.

134. 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.

<u>COUNT IX: UNJUST ENRICHMENT/QUANTUM MERUIT</u>
Under Florida Common Law

135. Corellium re-alleges and incorporates by reference paragraphs 1-134 as if fully set forth herein.

136. This is an action for unjust enrichment/quantum meruit under Florida common law.

137. Apple's Security Bounty Program Policy is a policy, a proposed course of action, not a contract or agreement.

138. In September 2017, Corellium became a participant in Apple's bug bounty program.

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

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

141. Corellium conferred a benefit to Apple by submitting the following bugs to Apple:

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.

142. 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.

143. By using Corellium's submissions to correct and update its software, Apple accepted and retained the benefit conferred to it by Corellium.

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

145. The benefit conferred to Apple was substantial. Under the guidelines of Apple's bug bounty program, the total market value of these bugs is, at a minimum, $300,000.

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

147. 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.

COUNT X: UNLAWFUL BUSINESS PRACTICE: UNJUST ENRICHMENT/QUANTUM MERUIT
Violation of Cal. Bus. & Prof. Code § 17200, *et seq.*

148. Corellium re-alleges and incorporates by reference paragraphs 1-147 as if fully set forth herein.

149. This is an action against Apple for unlawful business practices in violation of California Business & Professions Code § 17200, *et seq*.

150. Apple's bug bounty program is described in the document: "Apple Security Bounty Program Policy." This document is a policy, a proposed course of action—not a contract or agreement.

151. In September 2017, Corellium became a participant in Apple's bug bounty program.

152. As part of that program, Corellium submitted no fewer than seven bugs to Apple since November 2017.

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

154. 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.

155. 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.

156. It would be unjust for Apple to retain this benefit at Corellium's expense.

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

158. As alleged in Count VIII 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 & Professions Code § 17200, *et seq*.

159. As a direct result of Apple's actions, Corellium is entitled to restitution pursuant to California Business & Professions Code § 17203 in an amount to be proved at trial. In addition, Corellium seeks that the Court permanently enjoin Apple from engaging in the wrongful acts outlined in this Count. Finally, Corellium requests a declaration that Apple's actions as outlined in this Count constitute an unlawful business practice under California Business & Professions Code § 17200, *et seq*.

COUNT XI: IN THE ALTERNATIVE, BREACH OF CONTRACT
California Common Law

160. Corellium re-alleges and incorporates by reference paragraphs 1-159 as if fully set forth herein.

161. To the extent that Apple alleges that the Security Bounty Program Policy, other agreement, or some combination thereof govern the relationship between Apple and Corellium, and to the extent that the Court finds a binding and enforceable agreement between the parties, Corellium pleads that Apple breached any such agreement.

162. Specifically, Corellium pleads, in the alternative, that an agreement existed between Corellium and Apple pursuant to the Security Bounty Program Policy, another agreement, or combination thereof.

163. Pursuant to that agreement, Apple agreed to pay Corellium for bugs submitted by Corellium that conformed to the requirements specified in the agreement.

164. Corellium performed under the agreement by submitting the following bugs that conformed to the requirements specified in the agreement:

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.

165. Apple failed to pay Corellium for those submissions, which constitutes a material breach of the agreement between the parties.

166. Corellium did not receive payment for its work performed under the agreement. Apple's failure to pay Corellium for its submissions proximately caused Corellium's damages.

167. Corellium is therefore entitled to damages in the amount of the value of the bugs submitted which is not less than $300,000.

COUNT XII: IN THE ALTERNATIVE, BREACH OF CONTRACT
Florida Common Law

168. Corellium re-alleges and incorporates by reference paragraphs 1-167 as if fully set forth herein.

169. To the extent that Apple alleges that the Security Bounty Program Policy, other agreement, or some combination thereof govern the relationship between Apple and Corellium, and to the extent that the Court finds either to be a binding and enforceable agreement between the parties, Corellium pleads that Apple breached any such agreement.

170. Specifically, Corellium pleads, in the alternative, that a binding enforceable agreement existed between Apple and Corellium pursuant to the Security Bounty Program Policy, another agreement, or some combination thereof.

171. Pursuant to that agreement, Apple agreed to pay Corellium for bugs submitted by Corellium that conformed to the requirements specified in the agreement.

172. Corellium performed under the agreement by submitting the following bugs that conformed to the requirements specified in the agreement:

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.

173. Apple failed to pay Corellium for those submissions, which constitutes a material breach of the agreement between the parties.

174. Corellium did not receive payment for its work performed under the agreement. Apple's failure to pay Corellium for its submissions proximately caused Corellium's damages.

175. Corellium is therefore entitled to damages in the amount of the value of the bugs submitted which is not less than $300,000.

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 the award of any and all relief of any nature (*e.g.*, declaratory, monetary, equitable, or injunctive relief, interest, attorneys' fees, and costs) to which Corellium is entitled on its Counterclaims;

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

3. A judgment declaring that: (a) Apple's Security Bounty Program Policy is not an enforceable contract or agreement on its face, that any purported consideration is illusory, and that, therefore, there is no binding or enforceable agreement between Apple and Corellium pursuant to Apple's Security Bounty Program Policy; and (b) there is no binding or enforceable agreement between Apple and Corellium under the Security Bounty Program Policy, any other written agreement, or any combination thereof;

4. A judgment declaring that: (a) Apple's conduct as outlined in Count V constitutes an unlawful business practice in violation of California Business & Professions Code § 17200, *et seq.*; (b) Apple's conduct as outlined in Count VI constitutes an unfair business practice in violation of California Business & Professions Code § 17200, *et seq.*; (c) Apple's conduct as outlined in Count VII constitutes an unfair and/or deceptive trade practice in violation of Fla. Stat. § 501.201, *et. seq.*; and (d) Apple's conduct as outlined in Count X constitutes an unlawful business practice under California Business & Professions Code § 17200, *et seq.*;

5. A judgment ordering restitution against Apple for Apple's unlawful business practices and unfair business practices violating California Business & Professions Code § 17200, *et seq.*;

6. A judgment ordering damages against Apple for Apple's wrongful acts in violation of Fla. Stat. § 501.201, *et seq.*;

7. A judgment permanently enjoining Apple from engaging in unlawful business practices and unfair business practices violating California Business & Professions Code § 17200, *et seq.*;

8. A judgment permanently enjoining Apple from engaging in unfair and/or deceptive trade practices in violation of Fla. Stat. § 501.201 *et seq.*;

9. A judgment ordering attorneys' fees pursuant to Fla. Stat. § 501.2105 against Apple for Apple's unfair and/or deceptive trade practices in violation of Fla. Stat. § 501.201, *et seq.*;

10. A judgment ordering damages against Apple for constructive fraud;

11. A judgment ordering restitution against Apple for Apple's unlawful business practices in violation of California Business & Professions Code § 17200, *et seq.*;

12. A judgment ordering restitution against Apple for Apple's unjust enrichment/quantum meruit;

13. Or, in the alternative, a judgment ordering damages for Apple's breach of contract, should the Court determine a contract exists and is binding and enforceable on the parties;

14. A judgment ordering prejudgment interest and court costs; and

15. Such other equitable relief 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 January 10, 2020, 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 B. Levine
JONATHAN VINE
Florida Bar No.: 10966
JUSTIN LEVINE
Florida Bar No.: 106463
LIZZA CONSTANTINE
Florida Bar No.: 1002945