Paul J. Riehle (SBN 115199)
paul.riehle@faegredrinker.com
FAEGRE DRINKER BIDDLE & REATH LLP
Four Embarcadero Center
San Francisco, California 94111
Telephone: (415) 591-7500
Facsimile: (415) 591-7510

Christine A. Varney (*pro hac vice pending*)
cvarney@cravath.com
Katherine B. Forrest (*pro hac vice pending*)
kforrest@cravath.com
Gary A. Bornstein (*pro hac vice pending*)
gbornstein@cravath.com
Yonatan Even (*pro hac vice pending*)
yeven@cravath.com
M. Brent Byars (*pro hac vice pending*)
mbyars@cravath.com
CRAVATH, SWAINE & MOORE LLP
825 Eighth Avenue
New York, New York 10019
Telephone: (212) 474-1000
Facsimile: (212) 474-3700

Attorneys for Plaintiff Epic Games, Inc.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

EPIC GAMES, INC., Plaintiff, vs. APPLE INC., Defendant.	Case No. _____ **COMPLAINT FOR INJUNCTIVE RELIEF**

TABLE OF CONTENTS

NATURE OF THE ACTION 1
PARTIES 8
JURISDICTION AND VENUE 10
INTRADISTRICT ASSIGNMENT 12
RELEVANT FACTS 12
I. Apple Monopolizes the iOS App Distribution Market. 12
A. The iOS App Distribution Market. 16
B. Apple's Monopoly Power in the iOS App Distribution Market. 17
C. Apple's Anti-competitive Conduct in the iOS App Distribution Market 19
i. Technical Restrictions 19
ii. Contractual Restrictions 19
iii. Lack of Procompetitive Justification 22
D. Anti-competitive Effects in the iOS App Distribution Market. 23
II. Apple Monopolizes the iOS In-App Payment Processing Market. 27
A. The iOS In-App Payment Processing Market. 28
B. Apple's Monopoly Power in the iOS In-App Payment Processing Market 30
C. Apple's Anti-competitive Conduct in the iOS In-App Payment Processing Market. 32
i. Contractual and Policy Restrictions 32
ii. Lack of Procompetitive Justification 33
D. Anti-competitive Effects in the iOS In-App Payment Processing Market 34
III. Competition in the Sale of Mobile Devices Cannot Discipline Apple's Conduct in the iOS App Distribution or iOS In-App Payment Processing Markets. 38
A. Apple's Mobile Device Customers Face Substantial Switching Costs and iOS Lock-In. 38
B. Apple's Sticky iOS Ecosystem Protects its Dominance in the Sales of Mobile Devices 42

C. Information Costs and Other Market Inefficiencies in the iOS App Distribution and iOS In-App Payment Processing Markets. 44

COUNT 1: Sherman Act § 2 (Unlawful Monopoly Maintenance in the iOS App Distribution Market) 47

COUNT 2: Sherman Act § 2 (Denial of Essential Facility in the iOS App Distribution Market) 48

COUNT 3: Sherman Act § 1 (Unreasonable Restraints of Trade in the iOS App Distribution Market) 49

COUNT 4: Sherman Act § 2 (Unlawful Monopoly Maintenance in the iOS In-App Payment Processing Market) 51

COUNT 5: Sherman Act § 1 (Unreasonable Restraints of Trade in the iOS In-App Payment Processing Market) 52

COUNT 6: Sherman Act § 1 (Tying the App Store in the iOS App Distribution Market to In-App Purchase in the iOS In-App Payment Processing Market) 53

COUNT 7: California Cartwright Act (Unreasonable Restraints of Trade in the iOS App Distribution Market) 55

COUNT 8: California Cartwright Act (Unreasonable Restraints of Trade in the iOS In-App Payment Processing Market) 56

COUNT 9: California Cartwright Act (Tying the App Store in the iOS App Distribution Market to In-App Purchase in the iOS In-App Payment Processing Market) 58

COUNT 10: California Unfair Competition Law 61

PRAYER FOR RELIEF 61

Plaintiff Epic Games, Inc. ("Epic"), by its undersigned counsel, alleges, with knowledge with respect to its own acts and on information and belief as to other matters, as follows:

NATURE OF THE ACTION

1. In 1984, the fledgling Apple computer company released the Macintosh—the first mass-market, consumer-friendly home computer. The product launch was announced with a breathtaking advertisement evoking George Orwell's *1984* that cast Apple as a beneficial, revolutionary force breaking IBM's monopoly over the computing technology market. Apple's founder Steve Jobs introduced the first showing of the 1984 advertisement by explaining, "it appears IBM wants it all. Apple is perceived to be the only hope to offer IBM a run for its money . . . . Will Big Blue dominate the entire computer industry? The entire information age? Was George Orwell right about 1984?"

2. Fast forward to 2020, and Apple has become what it once railed against: the behemoth seeking to control markets, block competition, and stifle innovation. Apple is bigger, more powerful, more entrenched, and more pernicious than the monopolists of yesteryear. At a market cap of nearly $2 trillion, Apple's size and reach far exceeds that of any technology monopolist in history.

3. This case concerns Apple's use of a series of anti-competitive restraints and monopolistic practices in markets for (i) the distribution of software applications ("apps") to users of mobile computing devices like smartphones and tablets, and (ii) the processing of consumers' payments for digital content used within iOS mobile apps ("in-app content"). Apple imposes unreasonable and unlawful restraints to completely monopolize both markets and prevent software developers from reaching the over one billion users of its mobile devices (*e.g.*, iPhone and iPad) unless they go through a single store controlled by Apple, the App Store, where Apple exacts an oppressive 30% tax on the sale of every app. Apple also requires software developers who wish to sell

digital in-app content to those consumers to use a single payment processing option offered by Apple, In-App Purchase, which likewise carries a 30% tax.

4. In contrast, software developers can make their products available to users of an Apple personal computer (*e.g.*, Mac or MacBook) in an open market, through a variety of stores or even through direct downloads from a developer's website, with a variety of payment options and competitive processing fees that average 3%, a full ***ten times*** lower than the exorbitant 30% fees Apple applies to its mobile device in-app purchases.

5. The anti-competitive consequences of Apple's conduct are pervasive. Mobile computing devices (like smartphones and tablets)—and the apps that run on those devices—have become an integral part of people's daily lives; as a primary source for news, a place for entertainment, a tool for business, a means to connect with friends and family, and more. For many consumers, mobile devices are their primary computers to stay connected to the digital world, as they may not even own a personal computer. When these devices are unfairly restricted and extortionately "taxed" by Apple, the consumers who rely on these mobile devices to stay connected in the digital age are directly harmed.

6. Epic brings this suit to end Apple's unfair and anti-competitive actions that Apple undertakes to unlawfully maintain its monopoly in two distinct, multibillion dollar markets: (i) the iOS App Distribution Market, and (ii) the iOS In-App Payment Processing Market (each as defined below). Epic is not seeking monetary compensation from this Court for the injuries it has suffered. Nor is Epic seeking favorable treatment for itself, a single company. Instead, Epic is seeking injunctive relief to allow fair competition in these two key markets that directly affect hundreds of millions of consumers and tens of thousands, if not more, of third-party app developers.

7. Apple imposes unreasonable restraints and unlawfully maintains a total monopoly in the iOS App Distribution Market. To live up to its promise to users that "there's an app for that", Apple, after a short initial attempt to go it alone, opened up

iOS and invited third-party app developers to develop a wide array of apps for the iOS ecosystem. Those apps contribute immense value to that ecosystem and are one of the primary marketing features for iPhones and iPads. But Apple completely bans innovation in a central part of this ecosystem, namely, any app that could compete with Apple for the distribution of apps in iOS. Through its control over iOS, and through a variety of unlawful contractual restrictions that it forces app developers to accept, Apple prevents iOS users from downloading any apps from any source other than Apple's own storefront, the App Store.

8. The result is that developers are prevented from selling or distributing iOS apps unless they use Apple's App Store, and accede to Apple's oppressive terms and conditions for doing so (some of which are discussed further below). For example, as the sole distributor of iOS apps, Apple collects the money from every iOS user's app purchase, remits only 70% of that payment to the app developer, and retains a 30% tax for itself. iOS developers are thus forced to increase the prices they charge consumers in order to pay Apple's app tax. There is no method app developers can use to avoid this tax, as Apple has foreclosed any alternative ways to reach the over one *billion* users of iOS devices. As Representative Hank Johnson aptly summed up at a recent Congressional hearing on technology monopolies: "developers have no choice but to go along with [Apple's policies] or they must leave the App Store. That's an enormous amount of power."

9. Apple's anti-competitive conduct with respect to iOS app distribution results in sweeping harms to (i) app distributors, who are foreclosed from competing with Apple and innovating new methods of distributing iOS apps to users outside the App Store (such as, for example, curated app stores targeting particular categories of apps, like gaming or travel); (ii) app developers, who are denied choice on how to distribute their apps, are forced to fork over more of their revenue on paid apps than they would if Apple faced competition, and on occasion have to abandon their apps altogether if they cannot earn a profit given Apple's 30% tax; and (iii) consumers, who are likewise denied choice

and innovation in app distribution channels and are forced to pay higher prices and suffer inferior customer service from Apple, the unwelcome middleman. (Part I.)

10. Apple also imposes unreasonable restraints and unlawfully maintains a total monopoly in the iOS In-App Payment Processing Market. Among the oppressive terms that app developers have to accept, Apple coerces all app developers who wish to use its App Store—the only means with which to distribute apps to iOS users—to use exclusively Apple's own payment processing platform for all in-app purchases of in-app content. Apple thus requires third-party app developers to agree they will not even offer iOS users the *choice* of additional payment processing options *alongside* Apple's. And Apple goes as far as to gag app developers, preventing them from even *mentioning* to users the option of buying the same content outside of the app—for example, by purchasing content directly from the app developer, or using a web browser. Because Apple has a monopoly over the distribution of iOS apps, app developers have no choice but to assent to this anti-competitive tie; it is Apple's way or the highway.

11. In this market too, Apple thus stands as the monopolist middleman, positioning itself between developers and consumers. As the sole payment processor, Apple is able to take an exorbitant 30% fee on all in-app purchases of in-app content.

12. Apple's anti-competitive conduct with respect to iOS in-app payment processing harms: (i) other payment processors, who are foreclosed from competing with Apple on price and innovating new methods of in-app payment processing (such as, for example, rewards points or payment through carrier billing); (ii) app developers, who are denied choice on how to process payments and the benefits of innovation in payment processing, and are forced to pay Apple's tax—set by fiat—rather than by competitive market forces; and (iii) consumers, who are also denied choice and innovation in payment processing and suffer higher prices and inferior service. (Part II.)

13. Apple's anti-competitive conduct in these markets is unchecked; Apple faces little, if any, constraint on its monopoly power in both the iOS App Distribution and iOS In-App Payment Processing Markets, as Apple has foreclosed all

direct competition in these markets. And Apple stands as the sole middleman between a vast and dispersed group of iOS users, and a vast and dispersed group of app developers, each with little power individually to constrain Apple.

14. Further, competition in the sale of mobile devices does not limit Apple's market power. The threat of users switching to non-iOS devices does not constrain Apple's anti-competitive conduct because Apple's mobile device customers face significant switching costs and lock-in to the Apple iOS ecosystem, which serves to perpetuate Apple's substantial market power. This power manifests itself in the data, as Apple is able to gobble up over *two thirds* of the total global smartphone operating profits. Furthermore, when making mobile device purchases, consumers are either unaware of, or cannot adequately account for, Apple's anti-competitive conduct in the downstream app distribution and payment processing markets. The cost of app downloads and in-app purchases will play an insignificant (if any) role in swaying a consumer's smartphone purchase decision. (Part III.)

15. Epic is one of the many app developers affected by Apple's anti-competitive conduct. Epic is a developer of entertainment software for personal computers, smart mobile devices and gaming consoles. The most popular game Epic currently makes is *Fortnite*, which has connected hundreds of millions of people in a colorful, virtual world where they meet, play, talk, compete, dance, and even attend concerts and other cultural events. *Fortnite* is beloved by its millions of users. In the first year after *Fortnite*'s release in 2017, the game attracted over 125 million players; in the years since, *Fortnite* has topped 350 million players and has become a global cultural phenomenon.

16. Epic—and *Fortnite*'s users—are directly harmed by Apple's anti-competitive conduct. But for Apple's illegal restraints, Epic would provide a competing app store on iOS devices, which would allow iOS users to download apps in an innovative, curated store and would provide users the choice to use Epic's or another third-party's in-app payment processing tool. Apple's anti-competitive conduct has also

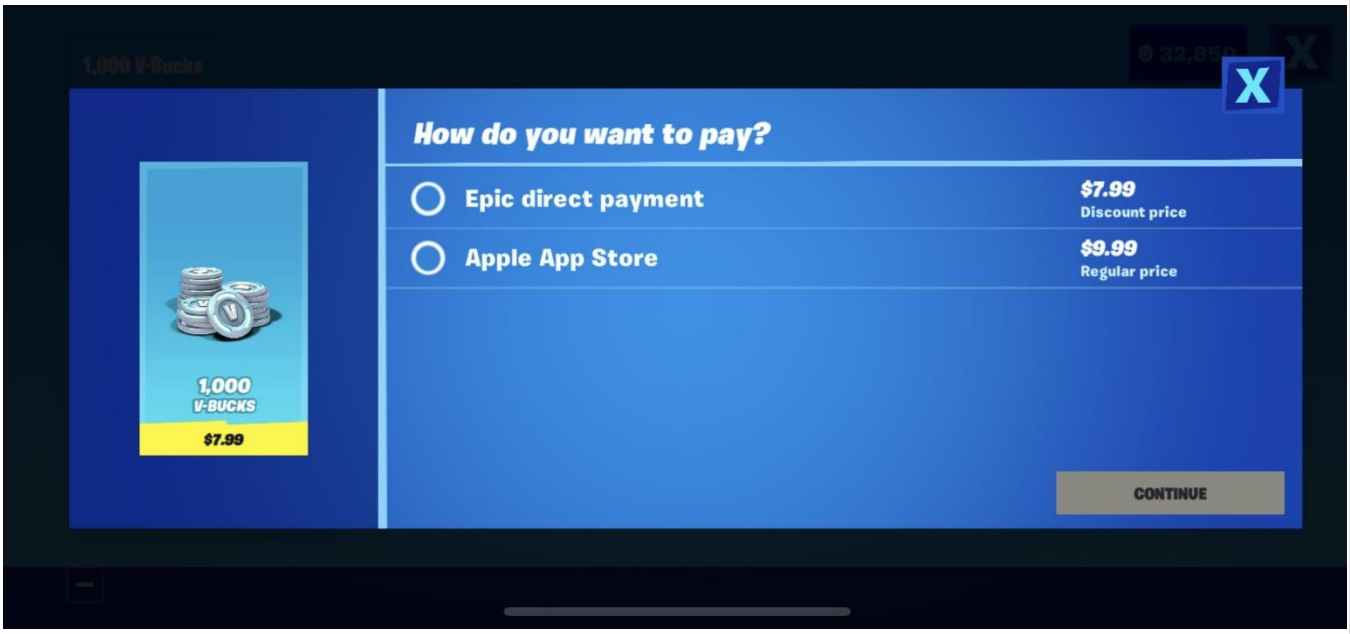
injured Epic in its capacity as an app developer by forcing Epic to distribute its app exclusively through the App Store and exclusively use Apple's payment processing services. As a result, Epic is forced, like so many other developers, to charge higher prices on its users' in-app purchases on *Fortnite* in order to pay Apple's 30% tax.

17. Contrast this anti-competitive harm with how similar markets operate on Apple's own Mac computers. Mac users can download virtually any software they like, from any source they like. Developers are free to offer their apps through the Mac computer App Store, a third-party store, through direct download from the developer's website, or any combination thereof. Indeed, on Macs, Epic distributes *Fortnite* through its own storefront, which competes with other third-party storefronts available to Mac users. App developers are free to use Apple's payment processing services, the payment processing services of third parties, or the developers' own payment processing service; users are offered their *choice* of different payment processing options (*e.g.*, PayPal, Amazon, and Apple). The result is that consumers and developers alike have choices, competition is thriving, prices drop, and innovation is enhanced. The process should be no different for Apple's mobile devices. But Apple has chosen to make it different by imposing contractual and technical restrictions that prevent any competition and increase consumer costs for every app and in-app content purchase—restrictions that it could never impose on Macs, where it does not enjoy the same dominance in the sale of devices. It doesn't have to be like this.

18. Epic has approached Apple and asked to negotiate relief that would stop Apple's unlawful and unreasonable restrictions. Epic also has publicly advocated that Apple cease the anti-competitive conduct addressed in this Complaint. Apple has refused to let go of its stranglehold on the iOS ecosystem.

19. On the morning of August 13, 2020, for the first time, Apple mobile device users were offered competitive choice. Epic added a direct payment option to *Fortnite*, giving players the *option* to continue making purchases using Apple's payment processor or to use Epic's direct payment system. *Fortnite* users on iOS, for the first

time, had a competitive alternative to Apple's payment solution, which in turn enabled Epic to pass along its cost savings by offering its users a 20% reduction in in-app prices as shown below:



20. Rather than tolerate this healthy competition and compete on the merits of its offering, Apple responded by removing *Fortnite* from sale on the App Store, which means that new users cannot download the app, and users who have already downloaded prior versions of the app from the App Store cannot update it to the latest version. This also means that *Fortnite* players who downloaded their app from the App Store will not receive updates to *Fortnite* through the App Store, either automatically or by searching the App Store for the update. Apple's removal of *Fortnite* is yet another example of Apple flexing its enormous power in order to impose unreasonable restraints and unlawfully maintain its 100% monopoly over the iOS In-App Payment Processing Market.

21. Accordingly, Epic seeks injunctive relief in court to end Apple's unreasonable and unlawful practices. Apple's conduct has caused and continues to cause Epic financial harm, but as noted above, Epic is not bringing this case to recover these damages; Epic is not seeking any monetary damages. Instead, Epic seeks to end Apple's

dominance over key technology markets, open up the space for progress and ingenuity, and ensure that Apple mobile devices are open to the same competition as Apple's personal computers. As such, Epic respectfully requests this Court to enjoin Apple from continuing to impose its anti-competitive restrictions on the iOS ecosystem and ensure 2020 is not like "1984".

PARTIES

22. Plaintiff Epic is a Maryland corporation with its principal place of business in Cary, North Carolina. Epic's mission is "to create fun games we want to play and to build the art and tools needed to bring those games to life".

23. Epic was founded in 1991 by a college student named Tim Sweeney who was studying mechanical engineering. Mr. Sweeney ran Epic out of his parents' garage and distributed by mail Epic's first commercial personal computer software, a game named *ZZT*. Since then, Epic has developed several popular entertainment software products that can be played on an array of platforms—such as personal computers, gaming consoles, and mobile devices.

24. Currently, Epic's most popular game is *Fortnite*, which has connected hundreds of millions of people in a colorful virtual world where they meet, play, talk, compete, dance, and even attend concerts and other cultural events.

25. Although some video games or other apps require users to pay before they download and use the software, *Fortnite* is free to download and play. Epic generates revenue by offering users various in-app purchases of in-app content. For example, players who wish to further express themselves within *Fortnite* through digital avatars, costumes, dances, or other cosmetic enhancements may purchase them within the *Fortnite* app. Through this model, Epic makes *Fortnite* widely accessible at no cost to consumers, while earning a return on its artistic and engineering investments through the sale of cosmetic enhancements.

26. *Fortnite* has become a global phenomenon. As noted, in the first year after *Fortnite* was released in 2017, the game attracted over 125 million players; in the years since, *Fortnite* has topped 350 million players and has become a global cultural phenomenon.

27. Epic also built and runs the Epic Games Store, a digital video game storefront through which gamers can download various games, some developed by Epic, and many offered by third-party game developers. The Epic Games Store is currently available on personal computers. Epic distributes *Fortnite* to users of personal computers—including users of Apple's own Mac computers—through the Epic Games Store. Epic also distributes other developers' games for a modest fee through the Epic Games Store. Worldwide, approximately 400 million users have signed up to play Epic's games, and each day 30 to 40 million individuals log into an Epic game.

28. Epic creates and distributes the *Unreal Engine*, a powerful software suite that allows users to create realistic three-dimensional content including video games, architectural recreations, television shows, and movies. An Epic subsidiary also develops and distributes the popular *Houseparty* app, which enables video chatting and social gaming on mobile devices and personal computers.

29. Defendant Apple is a California corporation with its principal place of business in Cupertino, California. Apple is the largest public company in the world, with a current market capitalization of close to $2 trillion. Apple designs, markets and sells smartphones (including the iPhone), personal computers (including Macs), tablets (including the iPad), wearables and accessories, and sells a variety of related services. Apple also owns and operates the Apple App Store (the "App Store"), including contracting with all app developers that distribute their apps through the App Store and is therefore a party to the anti-competitive contractual restrictions at issue in this Complaint.

JURISDICTION AND VENUE

30. This Court has subject matter jurisdiction over Epic's federal antitrust claims pursuant to the Clayton Antitrust Act, 15 U.S.C. § 26, and 28 U.S.C. §§ 1331

and 1337. The Court has supplemental jurisdiction over Epic's state law claims pursuant to 28 U.S.C. § 1367. The Court also has subject matter jurisdiction over the state law claims pursuant to 28 U.S.C. § 1332 based on the diversity of citizenship of Epic, on one hand, and of Apple, on the other. Although Epic does not seek monetary damages, the amount in controversy exceeds $75,000.

31. This Court has personal jurisdiction over Apple. Apple is headquartered in this District. Also, Apple has engaged in sufficient minimum contacts with the United States and has purposefully availed itself of the benefits and protections of both United States and California law such that the exercise of jurisdiction over Apple would comport with due process requirements.

32. Further, Apple has consented to the exercise of personal jurisdiction by this Court. Apple is party to an Apple Developer Program License Agreement (the "Developer Agreement") with Epic. Section 14.10 of the Developer Agreement provides that "[a]ny litigation or other dispute resolution" between the parties "arising out of or relating to this Agreement, the Apple Software, or Your relationship with Apple will take place in the Northern District of California", and that the parties "consent to the personal jurisdiction of and exclusive venue in the state and federal courts within" the Northern District of California. Section 14.10 further provides that the Developer Agreement "will be governed by and construed in accordance with the laws of the United States and the State of California". At least some of the claims raised in this Complaint "relate to" Epic's relationship with Apple.

33. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Apple maintains its principal place of business in the State of California and in this District, and because a substantial part of the events or omissions giving rise to Epic's claims occurred in this District. In the alternative, personal jurisdiction and venue also may be deemed proper under Section 12 of the Clayton Antitrust Act, 15 U.S.C. § 22, because Apple may be found in or transacts business in this District.

INTRADISTRICT ASSIGNMENT

34. Pursuant to Civil Local Rule 3-2(c), this antitrust case shall not be assigned to a particular Division of this District, but shall be assigned on a District-wide basis.

RELEVANT FACTS

I. Apple Monopolizes the iOS App Distribution Market.

35. To understand how Apple maintains a complete monopoly over the iOS App Distribution Market, it will be helpful to provide a background on smart mobile devices and Apple's control over key aspects of the devices.

36. Apple designs, markets, and sells mobile computing devices including smartphones, which it brands as iPhones, and tablets, which it brands as iPads. Smartphones and tablets are portable electronic devices that can connect wirelessly to the internet and are capable of multipurpose computing functions, including, among other things, internet browsing, sending and receiving email, accessing workplace software, editing documents, using social media, streaming video, listening to music, or playing games.

37. Similar to laptop and desktop personal computers, mobile devices such as smartphones and tablets require an operating system or "OS" that enables multipurpose computing functionality. An OS for mobile devices (a "mobile OS"), just like the OS of any computer, is a piece of software that provides basic functionality to users of smartphones, such as button controls, touch commands, motion commands, and the basic "graphical user interface", which includes "icons" and other visual elements representing actions that the user can take. A mobile OS also facilitates the basic operations of a smartphone, such as GPS positioning, camera and video recording, speech recognition and other features. In addition, a mobile OS permits the installation and operation of apps that are compatible with the particular OS.

38. Just as personal computers are sold to users with an OS pre-installed (*e.g.*, Microsoft Windows or macOS), smartphones and tablets are sold to users with a

mobile OS pre-installed. Mobile device suppliers, commonly known in the industry as original equipment manufacturers ("OEMs"), such as Samsung or Motorola, will select and install an OS prior to shipping their respective devices for sale.

39. The vast majority of OEMs do not develop or own a proprietary mobile OS, and must instead license a mobile OS for installation on their devices. The overwhelming majority of mobile devices sold by these OEMs use the Android OS, which is licensed by Google. In contrast, Apple uses a proprietary operating system called iOS, which it installs on the iPhone.[1] All iPhones and iPads are shipped with iOS pre-installed. Apple does not license or install any other mobile OS onto the iPhone or iPad, nor does it license iOS to any other OEM for installation on devices other than Apple's.

40. Thus, for mobile device users, there are effectively only two mobile operating systems to choose from: Google's Android OS or Apple's iOS. As of July 2020, these two operating systems accounted for nearly 100% of the worldwide mobile OSs.[2]

41. Mobile device users, including iOS device users, desire and use a number of apps in connection with their devices. Apps—software programs designed to run on smartphones and tablets—facilitate and magnify the full range of the device's functionality. For example, apps support consumers' shopping, social networking, food ordering and delivery, personal email, newspaper subscriptions, video and music streaming, or playing mobile games like *Fortnite*. Smartphones and tablets are also a ubiquitous tool for conducting business, and many consumers consult work calendars,

---

[1] Historically, iOS was also the operating system used on iPads. In 2019, Apple announced that it would begin using the name iPadOS to refer to the operating system on iPads. For simplicity's sake, this Complaint refers to the operating system on both devices as "iOS". There are no differences between iOS and iPadOS that are relevant to the allegations herein.

[2] StatCounter, "Mobile Operating System Market Share Worldwide", available online at https://gs.statcounter.com/os-market-share/mobile/worldwide (last accessed Aug. 10, 2020); S. O'Dea "mobile operating systems' market share worldwide from January 2012 to December 2019", *Statista* (Feb. 28, 2020), available online at https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/.

draft work emails, edit work documents, and perform other work functions on their mobile device. The ability to access these smart functions "on the go" forms part of the distinct value-add of apps to many consumers and businesses. For instance, the portability of smartphones, in conjunction with certain apps, enable uses that could not be replicated by a desktop computer—*e.g.*, real-time GPS-based driving directions, entering meal orders tableside, processing payments at open-air markets and craft fairs, or taking photos and instantly posting them to social media. In short, apps permit the customization of a user's device to cater to the user's specific interests and needs.

42. When the iPhone was first launched in 2007, it supported only Apple's native designed apps, and did not offer users access to any apps developed by third parties. Apple quickly changed its policy, as just one year later, Apple released its new iPhone 3G model that opened up the iOS ecosystem to permit third-party developers to create new and innovative applications for iOS users.

43. Since opening up its iOS platform, and up to today, the vast majority of apps are developed and programmed by third-party developers, although Apple and Google, who control iOS and Android OS, respectively, also develop and distribute apps of their own. To reach iOS app consumers, and to make their investment into developing iOS apps profitable, app developers need to be able to distribute their iOS apps to users.

44. All software programs, such as apps, must be updated from time to time, either to add functions, to address technical issues, or to ensure compatibility with an OS that has been updated. App updates are important to the continued functionality and commercial viability of apps, as well as a means to make ongoing improvements to each app. Some updates resolve technical or programming issues—*e.g.*, a software fix to a bug that caused the app to crash or to ensure the app remains compatible with an OS update—while other updates are designed to introduce new functionality or content into an app to support continued interest in the app by its users—*e.g.*, an update to a bank app that adds the ability to deposit checks, a business suite that has added new functions for its customers' or employees, or an update to a game that introduces new challenges or

cosmetic features. Thus, in addition to a channel for initial distribution, app developers need a way to inform app users of updates to their apps, and a feasible means of disseminating those updates.

45. Apps are OS-specific; they must be programmed to function on the particular OS on which they will be downloaded and run. Thus, apps developed for Android OS cannot substitute for apps designed for iOS. Developers who wish to distribute an app to users of devices with different OSs must therefore code different versions of their app for distribution to the different sets of users. To reach iOS device users, developers must program an iOS-compatible version of their app.

46. The iOS userbase is enormous. There are nearly a billion iPhone users worldwide and over 1.5 billion active iOS devices, including both iPhones and iPads.[3] Typically, these users will use *only* iOS devices and will not also use mobile devices with a different OS. In addition to its size, the iOS user base is also uniquely valuable in that its user base spends twice as much money on apps as Android users.[4] This is consistent with Epic's experience, as the average iOS *Fortnite* user spends significantly more on in-app purchases than the average Android *Fortnite* user.

47. iOS users are therefore a "must have" market for app developers to compete in; an app developer that chooses to develop apps for Android but not iOS forgoes the opportunity to reach over one billion high-paying app users.

48. When Apple sells its iPhones and iPads, it chooses which apps to pre-install prior to the sale of the device to consumers, which Apple limits to its own apps, *i.e.*, third-party apps do not come pre-installed. However, Apple can neither anticipate

---

[3] Michael Potuck, "Apple hits 1.5 billion active devices with ~80% of recent iPhones and iPads running iOS 13", *9To5Mac* (Jan. 28, 2020), available online at https://9to5mac.com/2020/01/28/apple-hits-1-5-billion-active-devices-with-80-of-recent-iphones-and-ipads-running-ios-13/.

[4] Prachi Bhardwaj, "Despite Android's growing market share, Apple users continue to spend twice as much money on apps as Android users", *Business Insider* (Jul. 6, 2018), available online at https://www.businessinsider.com/apple-users-spend-twice-apps-vs-android-charts-2018-7#:~:text=Despite%20Android's%20growing%20market%20share,on%20apps%20as%20Android%20users&text=On%20top%20of%20that%2C%20Android,a%20distant%20second%20at%2014%25.

nor deliver the complete universe of apps that any particular iOS device purchaser may desire to use. Nor do consumers themselves know at the time they purchase a device the many different apps they will want to download. Some of the apps an iOS device user eventually installs may not even have been developed or released at the time the user purchased the device, as new apps are released daily. Thus, it would be impractical and imprudent for Apple to load its iOS device with a large number of pre-installed apps, many of which would be unwanted by consumers. Instead, consumers are able to customize their devices for their own needs and uses by choosing which apps to install.

49. Users therefore benefit from app distribution services, including services that allow users to find new apps they desire to download and that make new apps and app updates seamlessly available for download and update.

50. Part I.A below describes the market for distribution of apps on iOS devices. Part I.B explains Apple's monopoly power in the market, and Part I.C describes Apple's anti-competitive acts to maintain its monopoly in the market. Finally, Part I.D describes the harm to competition, including to would-be competing app distributors, app developers, and consumers.

A. The iOS App Distribution Market.

51. There is a relevant market for the distribution of apps compatible with iOS to users of iOS devices, the iOS App Distribution Market. This market is comprised of all of the channels through which apps may be distributed to iOS device users.

52. One channel for distributing apps is an app store. App stores allow consumers to easily browse, search for, access reviews on, purchase (if necessary), download, and install mobile apps using just the mobile device and an internet connection.

53. Non-iOS app stores are not part of the iOS App Distribution Market. Because app stores are OS-specific, they distribute only those apps compatible with the mobile OS on which the app store is used. iOS device users can use only an app store designed to run on iOS, and thus cannot substitute an app store designed to run on

Google's Android OS. Accordingly, app developers cannot distribute their apps to iOS users on a non-iOS app store—*i.e.*, non-iOS app stores do not substitute for iOS app stores from developers' or consumers' perspectives.

54. Stores distributing personal computer or gaming console software are also not part of the iOS App Distribution Market. Such stores are not compatible with iOS and do not offer iOS-compatible apps: for example, Steam is a popular outlet for distributing gaming software compatible with personal computers, but the software it distributes cannot run on an iOS device. A user cannot download mobile apps for use on an iOS device by using such non-iOS, non-mobile software distribution platforms.

55. The same is true even when an app or game, like *Fortnite*, is available for different types of platforms running different operating systems. Only the OS-compatible version of that software can run on a specific type of device or computer. Accordingly, as a commercial reality, an app developer that wishes to distribute mobile apps for iOS devices must develop an iOS-specific version of the app and avail itself of the iOS App Distribution Market.

56. In the alternative only, the iOS App Distribution Market is a relevant, economically distinct sub-market of a hypothetical broader antitrust market for the distribution of mobile apps to users of all mobile devices, whether Apple's iOS or Google's Android OS.

57. The geographic scope of the iOS App Distribution Market is worldwide, as consumers and developers can access iOS worldwide.

B. Apple's Monopoly Power in the iOS App Distribution Market.

58. Apple has a monopoly in the iOS App Distribution Market. This is because the App Store is the ***sole means*** by which apps may be distributed to consumers in that market.

59. Apple's anti-competitive conduct (discussed in Part I.C below) forecloses all potential competitors from entering the iOS App Distribution Market. Apple prevents iOS users from downloading app stores or apps directly from websites;

pre-installs its App Store on every iOS device it sells; disables iOS users' ability to remove the App Store from their devices; and conditions all app developers' access to iOS on the developers' agreement to distribute their apps solely through the App Store and not to distribute third-party app stores. Although Apple could permit developers to build and offer competing iOS app stores, it denies all developers any opportunity to do so. Apple's power in the iOS App Distribution Market is absolute.

60. As a result of Apple's conduct, app developers have no choice but to offer apps exclusively through the App Store to reach the enormous userbase of iOS devices and are foreclosed from distributing apps by any other means.

61. ***Apple faces no constraints on its power*** in the iOS App Distribution Market. Non-iOS app distribution platforms do not constrain Apple's monopoly power in the iOS App Distribution Market because they are not compatible with iOS devices, they cannot provide iOS users with apps for their devices, and they do not contain iOS-compatible apps.

62. Nor can app developers constrain Apple's anti-competitive conduct in the iOS App Distribution Market by declining to develop apps for iOS. If a developer does not develop apps for iOS, the developer must forgo *all* of the over one billion or so iOS users. No developer alone has sufficient power to overcome the network effects and switching costs associated with iOS (*see* Part III below) to entice enough iOS users to leave iOS, such that developing apps solely for other platforms would be profitable. Thus, developers need to be on iOS.

63. Lastly, as described in Part III below, competition in the sale of mobile devices does not constrain Apple's power in the iOS App Distribution Market because iOS device users face substantial switching costs and lock-in to the iOS ecosystem. Further, regardless of the extent of competition in the sale of premium smartphones, competition at the smartphone level would not constrain Apple's power in the iOS App Distribution Market because consumers cannot adequately account for and

therefore constrain Apple's anti-competitive conduct through their purchasing behavior. The same is true for competition at the tablet level.

C. Apple's Anti-competitive Conduct in the iOS App Distribution Market.

64. Apple imposes unreasonable restraints and unlawfully maintains a monopoly in the iOS App Distribution Market through several anti-competitive acts, including technical restrictions (Part I.C.i below) and contractual restrictions. (Part I.C.ii below.) There is no procompetitive justification for these anti-competitive acts. (Part I.C.iii below.)

i. Technical Restrictions

65. Apple imposes several technical restrictions that foreclose competition in the iOS App Distribution Market.

66. *First*, Apple prevents iOS users from downloading app stores or apps directly from websites. Apple has done so by designing technical restrictions into iOS that prevent users from downloading app stores or apps directly from websites. As a result, iOS consumers must use Apple's App Store to download any apps to their devices, app developers must use Apple's App Store to distribute their apps to consumers, and would-be app distributors are unable to offer apps or competing app stores through their respective websites.

67. *Second*, Apple pre-installs its App Store on the home screen of every iOS device it sells. Apple does not pre-install (or even allow) any competing app stores anywhere on iOS devices. Apple also disables iOS users' ability to remove the App Store from their devices.

ii. Contractual Restrictions

68. Apple also imposes contractual restrictions that foreclose competition in the iOS App Distribution Market.

69. *First*, Apple conditions all app developers' access to iOS on the developers' agreement to distribute their apps solely through the App Store.

70. Apple effects this unlawful condition by requiring that all iOS developers enter into Apple's Developer Agreement, a contract of adhesion.

71. Section 3.2(g) of the Developer Agreement requires that developers distribute their apps only through the App Store. The Section provides that Applications "may be distributed only if selected by Apple (in its sole discretion) for distribution via the App Store, Custom App Distribution, for beta distribution through TestFlight, or through Ad Hoc distribution as contemplated in this Agreement".

72. The App Store is thus the only channel through which developers can distribute apps to the broad iOS userbase. Custom App Distribution, beta distribution through TestFlight, and Ad Hoc distribution are limited distribution channels that can only be used for specific types of commercial users.[5]

73. Custom App Distribution is available only in unique and specialized circumstances—namely, where a business or school needs to support the distribution and maintenance of apps on its devices. Custom App Distribution is the "store or storefront functionality that enables users to obtain Licensed Applications through the use of Apple Business Manager, Apple School Manager, or as otherwise permitted by Apple". (Developer Agreement § 1.2, Ex. A.) Organizations can use Apple Business Manager and Apple School Manager to organize their devices, apps, and accounts. These programs enable organizations to buy and distribute apps and content in bulk to their members or employees. Custom App Distribution does not allow developers to distribute apps to the broad iOS userbase; it is essentially a sanctioned extension of the App Store for narrow, specialized purposes, not a competing distribution channel.

74. Apple's beta testing program permits a developer to release non-final versions of apps through Apple's TestFlight Application to only a limited number of (i) the developer's own personnel and (ii) beta testers. (Developer Agreement § 7.4,

[5] Apple also allows certain Apple-approved large commercial organizations to participate in Apple's Developer Enterprise Program, which permits the approved organizations to develop and deploy proprietary, internal-use apps to their employees. This program does not permit developers to distribute apps to the broad iOS userbase.

Ex. A.) This program permits distribution only to a limited number of iOS devices (primarily owned and controlled by the developer) for the sole and specific purpose of facilitating the coding and testing of a developer's apps for use on the App Store; this program does not allow developers to distribute apps to the broad iOS userbase.

75. Ad Hoc distribution refers to the limited permission Apple gives a developer to distribute apps directly to the developer's own devices in connection with the developer's efforts to develop apps for iOS users. (Developer Agreement §§ 1.2, 7.3, Ex. A.) Because this permission is limited to a developer's devices and does not allow distribution to third parties, Ad Hoc distribution does not allow developers to distribute apps to the broad iOS userbase.

76. Therefore, by contractually conditioning developers' access to iOS on their agreement to distribute apps solely through the App Store, Apple further forecloses competition in the iOS App Distribution Market, as developers are contractually prevented from choosing to offer their iOS apps through third-party app stores.

77. *Second*, Apple conditions app developers' access to iOS on their agreement not to distribute third-party app stores.

78. Section 3.3.2(b) of the Developer Agreement prohibits "Application[s]" that "create a store or storefront for other code or applications".

79. Further, Apple's App Store Review Guidelines—which the Developer Agreement requires iOS developers to follow or risk removal from the App Store—make it "[u]nacceptable" to create "an interface for displaying third-party apps, extensions, or plug-ins similar to the App Store or as a general-interest collection". (App Store Review Guidelines § 3.2.2(i), Ex. B.)

80. In other words, to access the iOS userbase, app developers must agree not to distribute or create app stores that could compete with Apple's App Store—whether they intend to distribute their own app store through Apple's App Store or through the developer's own website.

81. Apple has enforced these restrictions against Epic. Epic approached Apple to request that Apple allow Epic to offer its Epic Games Store to Apple's iOS users through the App Store and direct installation. Apple's response was an unequivocal "no".

iii. Lack of Procompetitive Justification

82. There is no procompetitive justification for Apple's anti-competitive conduct in the iOS App Distribution Market.

83. Apple has asserted that blocking third-party app distribution platforms is necessary to enforce privacy and security safeguards. This is a pretext that Apple has used to foreclose *all* competition in the iOS App Distribution Market in which it has absolute monopoly power. A simple comparison to how Apple handles third-party software on its Mac personal computers illustrates how baseless its justifications are. Apple allows Mac users to access a number of different distribution channels to download software applications to their computers, including direct downloads from developer websites and the ability to purchase software applications from stores offered by third parties that compete with Apple's App Store. The consumer experience of acquiring software on Apple personal computers and Apple's smartphones is night and day. There is no legitimate reason why the same competitive structure for acquiring software on an Apple personal computer could not safely and securely exist on Apple's smart mobile devices.

84. There are a variety of mechanisms available to ensure the security of third-party applications that are less restrictive than prohibiting anyone other than Apple from distributing apps. If Apple believes it has a unique capability to screen apps for privacy and security issues, it could market those capabilities to competing app distributors, for a price. But if given the opportunity, competitors may be able to provide even *better* privacy and security safeguards. It is for users and the market to decide which store offers the best safeguards and at what price, not for Apple.

85. In describing the App Store for iOS, Apple claims to "believe competition makes everything better and results in the best apps for our customers".[6] Epic agrees. Competition in the iOS App Distribution Market would make everything better, and that includes better distribution services, better privacy and security safeguards, lower pricing, and access to apps that Apple currently and unfairly restricts.

86. Given the lack of any procompetitive justification, much less a sufficient one to justify the complete blocking of any competition, Apple's conduct imposes unreasonable restraints and unlawfully maintains its monopoly in the iOS App Distribution Market.

D. Anti-competitive Effects in the iOS App Distribution Market.

87. Apple's anti-competitive conduct forecloses competition in the iOS App Distribution Market, affects a substantial volume of commerce in this market, and causes anti-competitive harms to (i) would-be competing app distributors, (ii) developers, and (iii) consumers.

88. *First*, Apple's anti-competitive conduct harms all would-be app distributors by foreclosing them from competing in the iOS App Distribution Market.

89. But for Apple's restrictions, would-be competing app distributors, such as Epic, could develop and offer iOS-compatible app stores, thereby providing consumers and developers choice beyond Apple's own App Store and injecting healthy competition into the market. These stores could compete on the basis of (among other things) price, service and innovation. Competitors could innovate by (among other things) curating the apps available on a competing app store (such as offering selections of apps in particular categories of consumer interest, like gaming, travel, or health), providing more reliable reviews and other information about the apps, showing or advertising apps in different ways, or offering different pricing schemes.

[6] Apple, "App Store", https://www.apple.com/ios/app-store/principles-practices/ (last accessed Aug. 2, 2020).

90. For example, in the personal computer space (including Macs), software can be purchased through many different sellers, including special digital membership stores. In the gaming space, the leading store is Steam. To compete against Steam, Epic developed its own digital membership store to sell game software, the Epic Games Store. The Epic Games Store provides access to more than 250 games from more than 200 developers, and those numbers are growing rapidly. The Epic Games Store offers personalized features such as friends list management and game matchmaking services. Absent Apple's anti-competitive conduct, Epic would also create an app store for iOS.

91. Notable large technology companies have recently clashed with Apple and lost, demonstrating that Apple's monopoly power is not constrained by even large and well-capitalized market participants. As a result, iOS users are denied innovations. For example, on August 6, 2020, *The Verge* reported that a new and notable mobile gaming service, Microsoft's xCloud, would be launching its cloud-based online gaming system across a number of different platforms—but not on Apple's App Store.[7] Apple confirmed that it rejected xCloud for violating Apple's policies—the same policies described above that are designed to protect Apple's monopoly over the iOS App Distribution Market.[8] Microsoft expressed its discontent with the decision, stating that Apple is "stand[ing] alone as the only general purpose platform to deny consumers from cloud gaming and game subscription services like Xbox Game Pass".[9]

92. One day later, August 7, 2020, *The New York Times* reported that Facebook had unsuccessfully attempted for six months to obtain Apple's approval of a new Facebook Gaming app that would allow users to watch livestreams of online games

[7] Nick Statt, "Apple confirms cloud gaming services like xCloud and Stadia violate App Store guidelines" *The Verge* (Aug. 6, 2020), available online at https://www.theverge.com/2020/8/6/21357771/apple-cloud-gaming-microsoft-xcloud-google-stadia-ios-app-store-guidelines-violations.

[8] *Id.*

[9] *Id.*

and play simple games, like the popular Words With Friends.[10] Like it had with Microsoft, Apple unequivocally refused to allow Facebook to distribute its competing game store on the App Store.[11] Ultimately, Facebook caved under Apple's power and removed the ability for users to play games on its app, limiting it to a simple video streaming service.[12] As Facebook's vice president for gaming, Vivek Sharma, explained, Apple's conduct creates "shared pain across the games industry, which ultimately hurts players and developers and severely hamstrings innovation on mobile for other types of formats like cloud gaming".[13]

93. *Second*, Apple's anti-competitive conduct harms developers, including Epic.

94. Apple's conduct denies developers the choice of how best to distribute their apps. Developers are barred from reaching over one billion iOS users unless they go through Apple's App Store, and on Apple's terms. Developers cannot distribute their apps through competing app stores that could offer, for example, increased visibility or better or cheaper marketing. Nor can developers offer their apps directly though their own websites. Thus, developers are dependent on Apple's *noblesse oblige*, as Apple may deny access to the App Store, change the terms of access, or alter the tax it imposes on developers, all in its sole discretion and on the commercially devastating threat of the developer losing access to the entire iOS userbase.

95. Apple's total foreclosure of any competition in the iOS App Distribution Market reduces the competitive pressure for Apple to innovate and improve its own App Store, leaving developers with inferior distribution outlets compared to what

[10] Seth Schiesel, "Facebook Gaming Finally Clears Apple Hurdle, Arriving in App Store", *The New York Times* (Aug. 7, 2020), available online at https://www.nytimes.com/2020/08/07/technology/facebook-apple-gaming-app-store.html.

[11] *Id.*

[12] *Id.*

[13] *Id.*

would exist if competition were to drive further development and innovation in the market.

96. Apple's restrictions also prevent developers from experimenting with alternative app distribution models, such as providing apps directly to consumers, selling apps through curated app stores, selling app bundles, and more. By restricting developers in this way, Apple ensures that developers' apps will be distributed only on the App Store.

97. Additionally, Apple's conduct increases developers' costs. Apple is able to extract a supra-competitive 30% tax on purchases of paid apps. Developers require a reasonable return on their investment in order to dedicate the substantial time and financial resources it takes to develop an app. By imposing its 30% tax, Apple necessarily forces developers to suffer lower profits, reduce the quantity or quality of their apps, raise prices to consumers, or some combination of the three.

98. Apple itself has recognized that its tax is prohibitive to many app developers, because the 30% surcharge makes the development of many apps unprofitable. For example, in an internal discussion among Apple's top executives regarding Apple's 30% charge, Steve Jobs acknowledged that a developer cannot "buy/rent/subscribe from iOS without paying us [Apple], which we *acknowledge is prohibitive for many things*".[14]

99. *Third*, Apple's anti-competitive conduct harms consumers.

100. Apple's conduct denies consumers choice, as they are forced to obtain apps solely through the App Store, and Apple alone dictates which apps are available.

101. As explained above, the lack of any competition in the iOS App Distribution Market prevents innovation by foreclosing potential competing app stores and alternative app distribution channels, as well as reduces the competitive pressure for Apple to innovate and improve its own App Store or reduce its supra-competitive 30%

[14] E-mail from T. Cook, CEO, Apple, to Eddy Cue, VP of Internet Software and Services, Apple (Feb. 6, 2011) (emphasis added) (House Committee On the Judiciary: Online Platforms and Market Power, Apple Documents at HJC-APPLE-014816).

tax. Customers therefore are denied the opportunity to find and access apps by way of new, innovative distribution methods, including specialized app stores catering to their specific interests.

102. Additionally, Apple's conduct increases consumers' costs. Apple's market power permits it to impose a supra-competitive 30% tax on the price of apps purchased through the App Store—a rate that is far higher than what could be sustained under competitive conditions. Consumers bear some or all of that tax in the form of higher prices or reduced quantity or quality of apps.

II. Apple Monopolizes the iOS In-App Payment Processing Market.

103. Many app developers generate revenue by enabling purchases through their apps.

104. Epic's *Fortnite* is one such example. In *Fortnite*, players may purchase digital outfits, dance moves, and other cosmetic enhancements within the game.

105. Developers selling digital content, such as Epic, require some way by which consumers may seamlessly and efficiently make purchases in their apps.

106. To address the need for in-app payment processing, an application programming interface ("API") is integrated into apps. When a customer makes an in-app purchase, the API sends the customer's payment method (for example, a credit card) to a payment processor for approval, similar to how a customer at a brick-and-mortar store presents a payment method to a cashier for processing at a register. The payment processor processes the transaction and, if approved, indicates through the API that the app can make the purchased content available to the user.

107. There are a number of third-party payment processors such as Braintree, PayPal, Square, and Stripe. Alternatively, some developers, like Epic, have developed their own payment processing solutions. An app developer can select the payment processor (or combination of payment processors) that best enhances the user experience and helps facilitate a seamless, cost-effective, and efficient payment processing API to work within their apps.

108. On iOS, however, Apple eliminates any choice of in-app payment processors for in-app content and coerces developers into using Apple's In-App Purchase. Apple effects this unlawful tie by requiring developers who want to enable in-app sales of in-app content to use Apple's payment processor, exclusively—which forecloses any alternative payment processing solutions.

A. The iOS In-App Payment Processing Market.

109. There is a relevant market for the processing of payments for the purchase of digital content, including in-game content, that is consumed within iOS apps, the iOS In-App Payment Processing Market. The iOS In-App Payment Processing Market comprises the payment processing solutions that (but for Apple's unlawful conduct) iOS developers could turn to and integrate into their iOS-compatible apps to process in-app purchases of in-app content.

110. Absent Apple's unlawful conduct, app developers could integrate compatible payment processors into their apps to facilitate the purchase of in-app content. Developers also would have the capability to develop their own in-app payment processing functionality. And developers could offer users a choice among multiple payment processors for each purchase, just like a website or brick-and-mortar store can offer a customer the option of using Visa, MasterCard, Amex, Apple Pay, and more.

111. Apple offers separate payment solutions for the purchase of digital content than it does for other types of purchases, even within mobile apps. In-App Purchase can be used for the purchase of digital content for use in an app, while Apple offers a separate tool, Apple Pay, to facilitate the in-app purchase of physical products and services.

112. APIs and payment processing tools available outside of the app—such as transaction processing through a developer's website or over the phone—cannot substitute for in-app payment processing. The ability to process in-app transactions seamlessly and nearly instantaneously within the app itself provides immense benefits for app users and developers. For users, the need to go outside the app to complete a

purchase would severely disrupt the use of the app, especially in game situations like *Fortnite*, and would require substantially more effort to effectuate any purchase.

113. It is particularly important that app developers who sell in-app digital content be able to offer in-app transactions that are seamless, engrossing, quick, and fun. For example, a gamer who encounters a desirable "skin" within *Fortnite*, such as a Marvel superhero, may purchase it nearly instantly for a small price without leaving the app. Although *Fortnite* does not offer content that extends gameplay or gives players competitive advantages, other game developers offer such products—for example, "boosts" and "extra lives"—that extend and enhance gameplay. It is critical that such purchases can be made during gameplay itself, rather than in another manner. If a player were required to purchase game-extending extra lives outside of the app, the player may simply stop playing instead.

114. As another example, if a user of a mobile dating app encounters a particularly desirable potential dating partner, he/she can do more than "swipe right" or "like" that person, but can also purchase a digital item that increases the likelihood that the potential partner will notice his/her profile. If the user could not make that purchase quickly and seamlessly, he/she would likely abandon the purchase and may even stop "swiping" in the app altogether.

115. It is therefore essential that developers who offer digital content be able to seamlessly integrate a payment processing solution into the app, rather than requiring a consumer to go elsewhere, such as to a separate website, to process a transaction. Indeed, if an app user were directed to process a purchase of digital content outside of a mobile app, the user might abandon the purchase or stop interacting with the mobile app altogether

116. Mobile game developers particularly value the ability to provide users with engaging gameplay without imposing any burdens or distractions on consumers who wish to make in-app purchases. Developers would be harmed if their app users were directed to process their purchases outside of the app, as such users would likely reduce

their number of purchases, abandon purchases outright, or stop interacting with the app altogether. For these reasons, and in the alternative only, there is a relevant antitrust sub-market for processing purchases of virtual gaming products within mobile iOS games (the "iOS Games Payment Processing Market").

117. By contrast, app developers who sell physical products have multiple ways to process transactions, and consumers are more willing to use methods other than in-app purchases. For example, a consumer who desires to purchase a physical product from Amazon could readily use either Amazon's mobile app or Amazon's website, or could make the same or similar purchase in a number of other ways, including through another online seller or at a brick-and-mortar store.

118. The geographic scope of the iOS In-App Payment Processing Market is worldwide, as consumers and developers can access iOS worldwide. Further, Apple's 30% tax does not vary by locality.

B. Apple's Monopoly Power in the iOS In-App Payment Processing Market.

119. Apple has a monopoly over the iOS In-App Payment Processing Market and, in the alternative, over the iOS Games Payment Processing Market, as it has a 100% market share.

120. As explained in Part I above, Apple has a complete monopoly in the iOS App Distribution Market. As the gatekeeper to the App Store, Apple is able to unlawfully condition access to the App Store on iOS app developers' use of Apple's In-App Purchase to process all in-app payments for in-app content.

121. Additionally, through its exclusionary tactics in the iOS In-App Payment Processing Market (Part II.C below), Apple is able to maintain its monopoly over that market.

122. Apple does not face any meaningful constraints to its monopoly power in the iOS In-App Payment Processing Market. As discussed above, APIs and

payment processing tools available outside of iOS cannot substitute for in-app payment processing because they severely disrupt the use of the app.

123. Competition in the iOS App Distribution Market cannot constrain Apple in the iOS In-App Payment Processing Market because there is no such competition, as explained in Part I.

124. Nor can app developers constrain Apple's anti-competitive conduct in the iOS In-App Payment Processing Market by declining to develop apps for iOS. If a developer does not develop apps for iOS, the developer must forgo *all* of the one billion plus iOS users. No developer has sufficiently important or attractive apps to overcome the network effects and switching costs (*see* Part III below) associated with iOS to entice enough iOS users to leave iOS, such that developing apps solely for other platforms would be profitable. Thus, developers need to be on iOS.

125. Apple charges a 30% fee for In-App Purchase. This rate reflects Apple's market power and the lack of competition, which allow Apple to charge supra-competitive prices for payment processing within the market.

126. The cost of alternative electronic payment processing tools, which Apple does not permit to be used for the purchase of in-app digital content, can be ***one tenth*** of the cost of In-App Purchase.

Electronic Payment Processing Tool	**Base U.S. Rate**
PayPal	2.9%
Stripe	2.9%
Square	2.6%-3.5%
Braintree	2.9%

127. Lastly, as described in Part III below, competition in the sale of mobile devices does not constrain Apple's power in the iOS In-App Payment Processing Market because iOS device users face substantial switching costs and lock-in to the iOS ecosystem. Further, regardless of competition in the sale of mobile devices, competition

at the smartphone level would not constrain Apple's power in the iOS App Distribution Market because consumers cannot adequately account for and therefore constrain Apple's anti-competitive conduct through their purchasing behavior. The same is true of competition at the tablet level.

C. Apple's Anti-competitive Conduct in the iOS In-App Payment Processing Market.

128. Apple imposes unreasonable restraints and unlawfully maintains its monopoly in the iOS In-App Payment Processing Market through several anti-competitive acts, including contractual and policy restrictions on app developers. (Part II.C.i below.) There is no procompetitive justification for these anti-competitive acts. (Part II.C.ii below.)

i. Contractual and Policy Restrictions

129. Through its unlawful policies and restrictions, Apple unlawfully ties In-App Purchase to the use of its App Store and forecloses any potential competition in the iOS App Payment Processing Market.

130. Developers seeking to distribute their apps on the App Store are required to follow Apple's App Store Review Guidelines or risk Apple rejecting or removing their app from the App Store. (Developer Agreement § 6.3, Ex. A.) Section 3.1.1 of these guidelines provide that "if you [the developer] want to unlock features or functionality within your app, (by way of example: subscriptions, in-game currencies, game levels, access to premium content, or unlocking a full version), you ***must use in-app purchase***. Apps ***may not use their own mechanisms to unlock content or functionality*** . . . . Apps and their metadata may not include buttons, external links, ***or other calls to action that direct customers to purchasing mechanisms other than in-app purchase***". (emphases added).

131. Additionally, Section 3.1.3 of the guidelines provides that developers may not "directly or indirectly target iOS users to use a purchasing method ***other than [Apple's] in-app purchase***, and general communications [to users] about other

purchasing methods [must not be] ***designed to discourage use of [Apple's] in-app purchase***". (emphases added).

132. These guidelines enumerate Apple's anti-competitive tying policy: an app developer's access to the App Store—the only means to reach Apple's substantial iOS userbase—is conditioned on the developer's use of Apple's In-App Purchase to process payments for in-app content. But Apple's policies take it yet another step further, gagging developers from even *informing* users of other payment options outside the app or from discouraging its users from using Apple's payment system. These draconian policies serve to cement Apple's monopoly position in the iOS In-App Payment Processing Market.

133. Apple strictly enforces these contractual terms. For example, in an October 2016 letter from Apple's General Counsel to Spotify, Apple threatened to remove Spotify's app from the App Store for advertising free trials to its own customers.[15] Apple decreed: "What a developer cannot do is seek to use its iOS app as a marketing tool to redirect consumers outside of the app to avoid in-app purchase."[16]

134. Apple thus requires all developers to use its In-App Purchase to the exclusion of any third-party payment processing solution, foreclosing any would-be competing in-app payment processors from entering the iOS In-App Payment Processing Market. In other words, app developers are coerced into using In-App Purchase by virtue of wanting to use the App Store.

ii. Lack of Procompetitive Justification

135. Apple's foreclosure of the iOS In-App Payment Processing Market has no procompetitive justification.

136. There is no security justification for requiring the use of In-App Purchase for a user's in-app purchase of in-app content. The best illustration of this point

[15] Letter from Bruce Sewell, General Counsel, Apple, to Horacio Gutierrez, General Counsel, Spotify (Oct. 28, 2016) (House Committee On the Judiciary: Online Platforms and Market Power, Apple Documents at HJC-APPLE-013579).

[16] *Id*.

is Apple's own conduct. Apple does not require that its In-App Purchase be used for in-app purchases of physical goods and certain services that are consumed outside the app. There is no security-based distinction between purchases of such physical goods (*e.g.*, food, clothing) and services (*e.g.*, rideshares, lodging), on the one hand, and purchases of in-app content (*e.g.*, game content unlocks, character cosmetics), on the other. Apple permits app developers like Amazon, Uber and Airbnb to process payments from customers for the goods and services they sell; it can likewise permit Epic, Match, Pandora and others to process payments from customers for the digital goods and services they sell.

137. Moreover, the security of a payment processing system is an element on which payment processors can compete—and do compete in non-monopolized markets where alternatives are available. If Apple's payment processing is truly the most secure, Apple can make that case in a competitive market. Apple should not be permitted to shield itself from competition and simply declare itself the most secure; it is for consumers and the market, not Apple, to determine what payment processing service is best.

138. Apple has also asserted on occasion that it must force developers and consumers to use In-App Purchase so that Apple can monitor each transaction and ensure that Apple is paid. But this assertion is circular; it presupposes that Apple is entitled to take a cut of every in-app purchase of in-app content on an iOS device (though it does not make the same claim for its Mac personal computers or for other types of in-app purchases on iOS devices). Apple has no such entitlement. Apple can seek recompense for any services it provides without fencing out competition in in-app payment processing. It is market competition, not Apple's dictate, that should set the terms on which apps obtain in-app payment processing services.

D. Anti-competitive Effects in the iOS In-App Payment Processing Market.

139. Apple's anti-competitive conduct forecloses competition in the iOS In-App Payment Processing Market, affects a substantial volume of commerce in that

market, and causes anti-competitive harms to (i) would-be competing in-app payment processors, (ii) app developers, and (iii) consumers.

140. *First*, Apple's anti-competitive conduct forecloses all would-be in-app payment processors from competing in the iOS In-App Payment Processing Market.

141. But for Apple's restrictions, would-be competing in-app payment processors could offer alternative in-app payment processing tools, giving app developers and consumers choices beyond Apple's In-App Purchase, and spurring innovation, better service and lower prices. These innovations could include, for example, alternative means to pay for in-app purchases of in-app content—which Apple does not offer—such as billing to the customer's cellular carrier, using Bitcoin or other cryptocurrencies, offering rewards points to customers, or providing more than one in-app payment processor. Apple's anti-competitive conduct eliminates all of these innovations and alternative payment options.

142. For example, outside of the restricted iOS ecosystem, Epic has worked with a number of third-party payment companies that provide creative new forms of payment processing solutions for consumers. One such example is Skrill, which offers Epic's customers pre-paid "Paysafe" cards offered in convenience stores across Poland and Germany that can unlock in-game content. Absent Apple's anti-competitive conduct, developers could offer similar payment services on iOS.

143. *Second*, Apple's anti-competitive conduct harms developers, including Epic.

144. Apple's conduct denies developers innovation, which could be provided by would-be competing in-app payment processors, as explained above.

145. Apple's conduct also denies developers choice and coerces them to use Apple's In-App Purchase. Developers are contractually required to use Apple's in-App Purchase to facilitate in-app purchases of in-app content on their iOS apps—and no alternative third-party payment processor can be used.

146. But for Apple's restrictions, developers could choose other options. For example, Epic would offer its own payment processing service for *Fortnite*. Epic already does so on personal computers, including Macs.

147. Apple also harms app developers' relationship with their customers by inserting itself as a mandatory middleman in every in-app transaction. When Apple acts as payment processor, Epic is unable to provide users comprehensive customer service relating to in-app payments without Apple's involvement. Apple has little incentive to compete through improved customer service because Apple faces no competition and consumers often blame Epic for payment-related problems. In addition, Apple is able to obtain information concerning Epic's transactions with its own customers, even when Epic and its own customers would prefer not to share their information with Apple.

148. Additionally, Apple's conduct increases developers' costs. As noted, Apple extracts an exorbitant 30% tax on in-app purchases of in-app content. Developers require a reasonable return on their investment in order to dedicate the substantial time and financial resources it takes to develop an app. By imposing its 30% tax, Apple necessarily forces developers to suffer lower profits, reduce the quantity or quality of their apps, raise prices to consumers, or some combination of the three.

149. Notably, Apple's 30% charge on in-app purchases is much higher than fees charged by analogous electronic payment processors in competitive contexts, such as PayPal, Stripe, Square or Braintree, which typically charge payment processing rates of around 3%, a 10-fold decrease from Apple's supra-competitive rates.[17] As another example, Google charges 2.9% or less for the use of Google Pay, an electronic payment processor that Google makes available to app developers for processing payments for physical products sold on Android apps. If developers were able to rely on their own solutions, or those of third-party payment processors, they could offer users lower prices for in-app purchases—as well as better customer service and alternative

[17] Yowana Wamala, "Amazon Payments Review: Should Your Business Use it?", *Value Panguin* (June 11, 2019), https://www.valuepenguin.com/credit-card-processing/amazon-payments-review.

payment options. Apple could not maintain its 30% tax if it did not unlawfully foreclose competition.

150. A glimpse of these anti-competitive effects recently manifested as a result of the ongoing global coronavirus pandemic. ClassPass, a company that developed an app to help consumers book exercise classes at gyms, has historically avoided having to pay any tax to Apple, as its services related to in-person workout classes. After the pandemic began, however, ClassPass adapted to its customers' needs and began offering virtual workout classes for the many who were stuck at home. On July 28, 2020, The *New York Times* reported that, in response to this shift to digital classes, Apple asserted that ClassPass was now offering in-app content and demanded that ClassPass pay Apple the 30% tax on in-app purchases of the virtual classes. As a result of Apple's demands, ClassPass stopped offering its virtual classes on its app, depriving consumers the benefit of innovative content specifically designed to address their needs during this unprecedented time.

151. *Third*, Apple's anti-competitive conduct harms consumers.

152. Apple's conduct denies consumers innovation, which could be provided by would-be competing in-app payment processors, as explained above.

153. Apple's conduct also denies consumers choice, as they are forced to make in-app purchases of in-app content solely through Apple's In-App Purchase.

154. Further, as noted above, Apple undermines the quality of services that consumers receive because Apple stands as a middleman in every in-app purchase of in-app content. Developers, therefore, are unable to resolve customer complaints arising from in-app purchases directly. For example, Apple does not have a formal mechanism through which developers can determine why a particular refund went through or was rejected, thereby impeding developers' efforts to offer high-quality customer service to consumers.

155. Finally, Apple's conduct increases consumers' costs. Apple's market power permits it to impose an exorbitant 30% tax on in-app purchases of in-app content.

Consumers must bear some or all of that tax in the form of higher in-app content prices and/or reduced quantity or quality of in-app content.

III. Competition in the Sale of Mobile Devices Cannot Discipline Apple's Conduct in the iOS App Distribution or iOS In-App Payment Processing Markets.

156. Competition in the sale of mobile devices cannot constrain Apple's anti-competitive conduct described in Parts I and II.

157. *First*, Apple's power in the relevant markets described above is not disciplined by competition in the sale of mobile devices because Apple mobile device customers face significant switching costs and customer lock-in to Apple's iOS ecosystem. (Part III.A.) These conditions manifest themselves in Apple's ability to maintain its substantial power in the sale of premium smartphones and tablets. (Part III.B.)

158. *Second*, Apple's power in the relevant markets described above is not disciplined by competition in the sale of mobile devices because consumers cannot adequately account for, and therefore constrain, Apple's anti-competitive conduct through their device purchasing behavior. The cost of app downloads and in-app purchases—unknowable by the consumer at the time of a smartphone or tablet purchase, but likely far less than the price of the device itself—will play an insignificant (if any) role in swaying a consumer's mobile device purchasing decision. (Part III.C.)

A. Apple's Mobile Device Customers Face Substantial Switching Costs and iOS Lock-In.

159. Apple's power in the iOS App Distribution Market and iOS In-App Payment Processing Markets is not constrained by competition in the sale of mobile devices because Apple's mobile device customers face high switching costs and are locked in to Apple's ecosystem for at least six reasons. These costs make it more difficult for users to purchase a mobile device from a competitor after having committed to Apple's mobile devices, thereby bolstering Apple's market power.

160. *First*, consumers are deterred from leaving the iOS ecosystem because of the difficulty and costs of learning a new mobile operating system. Mobile operating

systems have different designs, controls, and functions. Customers who use one (and often more than one) Apple product learn to operate efficiently on Apple's specific operating systems. For example, the iOS layout differs from Android OS in a wide range of functions, including key features such as searching and installing widgets on the phone to organize and search the phone's digital content, configuring control center settings, and organizing photos. Learning to use a new mobile operating system is thus time-consuming and burdensome for many consumers.

161. *Second*, switching from Apple's iOS devices may cause a significant loss of personal and financial investment that consumers put into the iOS ecosystem. Consumers choose a mobile device based in part on the OS that comes pre-installed on that device and the ecosystem in which the device participates. Once a consumer has chosen a mobile device, the consumer cannot replace the mobile OS that comes pre-installed on it with an alternative mobile OS. Rather, a consumer who wishes to change the OS must purchase a new device entirely. And because apps, in-app content and many other products are designed for compatibility with a particular mobile OS, switching to a new mobile OS may mean losing access to such products or to data saved by such products. Even if versions of such apps and products are available within the new ecosystem chosen by the consumer, the consumer would have to go through the process of downloading them again onto the new devices and (for paid apps or paid content) may have to purchase some or all of these apps anew. As a result, the consumer may be forced to abandon his or her investment in at least some of those apps, along with any purchased in-app content and consumer-generated data on those apps.

162. *Third*, the switching costs are compounded by the fact that consumers typically commit to the iOS ecosystem on a household or Apple device user group basis. Apple encourages lock-in across users and families. For example, Apple allows family members to access the songs, movies, TV shows, books, and apps purchased by other family members. Further, apps like FaceTime (which enables video and audio communication), Find My (which enables users to share their physical locations),

iMessage (which enables instant messaging), and AirDrop (a simple way to share content between Apple devices) work only between Apple device users. Customers who might consider switching from an iPhone or iPad would lose access to these services that connect friends and family. The loss of these integrated services raises the personal and financial costs for one member of a household or group to go it alone on a separate mobile operating system.

163. *Fourth*, consumers typically commit to Apple's ecosystem by purchasing more than one Apple device, which further increases their investment in iOS. Consumers are more likely to buy an iPhone, for example, if they already have an iPad or other Apple device because of the complementary services Apple provides for its device users. In 2017, CNBC conducted a survey of Americans' ownership of Apple devices and found that while 64% of Americans own an Apple product, the average American household owns an average of 2.6 Apple devices. Apple has developed a number of services that work exclusively on Apple devices to facilitate the interaction between Apple devices and encourage multiproduct ownership. For example, Apple developed a multifeatured product, Continuity, which "make[s] it seamless to move between your [Apple] devices". Continuity allows an Apple device customer to perform numerous cross-Apple device sharing functions, such as Handoff (beginning work on an app in one device and quickly switching to continue the work on another), Universal Clipboard (copying content including text, images, and photos on one device to paste on another), Instant Hotspot (making a personal hotspot on one device available to other Apple devices), and AirDrop (wirelessly sending documents, photos, videos, map locations, and websites across Apple devices). A customer choosing to purchase or switch to a non-Apple device loses access to these services, leading to increased costs a customer must face when choosing to leave Apple's ecosystem.

164. *Fifth*, Apple provides services to facilitate upgrading from one generation of Apple devices to the next. For example, Apple hosts its own "iPhone Upgrade Program", which allows customers to make recurring payments over the course

of a year and "get a new iPhone every year". Apple facilitates the transfer of a user's data like contacts and photos from an old iPhone to a new iPhone with a "migration feature that lets you move your data from an old device to a new one via wireless or wired transfer". Although there are now third-party apps and Android OEMs that attempt to make the switch from Apple to Android phones easier for consumers, "these all-in-one [data transfer] methods aren't available for every phone, and they don't always work flawlessly or across all of the areas relevant to your needs."

165. *Sixth*, Apple's mobile devices are protected from competition by their central place in Apple's developed ecosystem. An ecosystem is the network of products and services, including apps and smartphone accessories, designed to be inter-dependent and compatible with the specific operating system that runs on a given mobile device. The iOS ecosystem participants include an array of stakeholders, such as Apple, developers of iOS-compatible apps, iPhone and iPad owners, the makers of ancillary hardware to connect to the smartphone and iPad (*e.g.*, headphones or speakers), cellular carriers, and others. Being connected to these ecosystems greatly increases the value of the mobile devices to its users, as the more investments that are made by the various stakeholders, the more benefits accrue to the goods and services connected to the network. Apple's iPhone and iPad customers therefore benefit from substantial network effects of being plugged into the iOS ecosystem. For example, the more developers that design useful apps for iOS, the more consumers will be drawn to use the mobile devices for which those apps are designed, which then increases the benefits to developers to participate in the iOS, which encourages customers to purchase or retain their iOS mobile devices, and so on and so forth in a positive feedback loop. Therefore, any potential business looking to compete in the sale of mobile devices must make significant investments and coordinate a wide range of stakeholders to duplicate the benefits of a sprawling ecosystem, and iPhone and iPad customers must attempt to calculate the costs of losing their place in the iOS ecosystem.

166. As a result, Apple customers are often stuck with large price increases and locked into the iOS ecosystem, as switching out of the ecosystem is prohibitively difficult and expensive for consumers.

B. Apple's Sticky iOS Ecosystem Protects its Dominance in the Sales of Mobile Devices.

167. Apple's ability to raise customer switching costs and create customer lock-in to its iOS ecosystem is reflected in Apple's ability to maintain its dominance in the sale of premium smartphones as well as in the sale of tablets.

168. *First*, Apple's iPhone dominates sales of premium smartphones.

169. In 2019 alone, Apple's global iPhone sales generated more than $142 billion in revenues.[18] And in the first quarter of 2020, Apple was able to capture approximately 60% of global premium smartphone revenue.[19]

170. Furthermore, in the first quarter of 2020, 57% of premium smartphones sold globally were iPhones; Apple's nearest competitor sold only 19%.[20]

171. Apple's iPhone durably maintains substantial profit margins. For instance, from 2013 to 2017, Apple's share of smartphone operating profits among major smartphones companies ranged from 62% to 90%.[21] Similarly, in the third quarter of 2019, Apple was able to capture 66% of the operating profits across all mobile handsets. Apple's closet competitor had only 17%.[22] Analysts who follow Apple have also noted

---

[18] Statista Research Department, "Apple's iPhone revenue from 3rd quarter 2007 to 3rd quarter 2020" (Aug. 7, 2020), *available online at* https://www.statista.com/statistics/263402/apples-iphone-revenue-since-3rd-quarter-2007/.

[19] IDC Data.

[20] Varun Mishra, "Four Out of Five Best Selling Models in the Premium Segment Were From Apple", *Counterpoint Research* (June 15, 2020), online at https://www.counterpointresearch.com/apple-captured-59-premium-smartphone-segment/ (last accessed on Aug. 2, 2020).

[21] Chuck Jones, "Apple Continues To Dominate The Smartphone Profit Pool", *Forbes* (Mar. 2, 2018), https://www.forbes.com/sites/chuckjones/2018/03/02/apple-continues-to-dominate-the-smartphone-profit-pool/#65fbdddf61bb.

[22] Karn Chauhan, "Apple Continues to Lead Global Handset Industry Profit Share", *Counterpoint Research* (Dec. 19, 2019), online at https://www.counterpointresearch.com/apple-continues-lead-global-handset-industry-profit-share/ (last accessed on Aug. 2, 2020).

that since its release in 2007, the iPhone has able to maintain substantial profit margins of between 60% to 74%.[23]

172. Apple has also been able to maintain its pricing power over many years. For example, the global average selling price of smartphones went from $332 in 2011[24] to $363 in the first quarter of 2018,[25] a slight 4.3% price increase. Meanwhile, the iPhone has consistently sold at an average selling price of around $300 dollars higher than the average smartphone, and its prices increased over that same period by 22%, from approximately $650 to $796.[26]

173. The high switching costs are also obvious from empirical evidence. According to a 2017 survey by Morgan Stanley, 92 percent of iPhone users intending to upgrade within the next year indicated they would stick to an iOS device.[27] Similarly, Consumer Intelligence Research Partners found that 91 percent of iOS users who activated a new or used phone in the final three months of 2018 upgraded to another iPhone.[28]

174. Apple's pricing conduct also evidences the high switching costs. For example, Apple released the top-of-the-line iPhone X in 2017 at a $300 higher price point

---

[23] Alan Friedman, "Apple's profit margin on the iPhone has fallen from a peak of 74% to 60% over the years", *PhoneArena* (Nov. 15, 2018), online at https://www.phonearena.com/news/Profit-margins-on-the-iPhone-have-fallen-to-60_id111023.

[24] Statista Research Department, "Global Average Selling Price of Smartphones from 2010 to 2019", *Statista* (June 16, 2015), online at https://www.statista.com/statistics/484583/global-average-selling-price-smartphones/ (last accessed Aug. 2, 2020).

[25] Rani Molla, "Why people are buying more expensive smartphones than they have in years", *Vox* (Jan 23, 2018), https://www.vox.com/2018/1/23/16923832/global-smartphone-prices-grew-faster-iphone-quarter.

[26] Felix Richter, "iPhone ASP Edges Closer to $800", *Statista* (Nov. 2, 2018), https://www.statista.com/chart/15379/iphone-asp/ (last accessed Aug. 2, 2020).

[27] Martin Armstrong, "Most iPhone Users Never Look Back, *Statista* (May 22, 2017), online at https://www.statista.com/chart/9496/most-iphone-users-never-look-back/ (last accessed July 29, 2020).

[28] Joe Rossignol, "CIRP says iOS Loyalty 'Hit the Highest Levels We've Ever Measured' Last Quarter", *MacRumors* (Jan. 28, 2019), online at https://www.macrumors.com/2019/01/28/cirp-iphone-android-loyalty-4q18/ (last accessed July 29, 2020).

than the previous model. This was not followed by any major exodus to non-iOS systems; instead, consumers generally accepted the new price point, reflecting consumers' reluctance to switch even in the face of very significant increases in direct prices.

175. *Second*, Apple maintains significant power in the sale of tablets.

176. Apple's global iPad sales generated more than $19 billion in revenue in 2019 alone.[29] And Apple led all tablet vendors worldwide, accounting for 38% of the global tablet shipments in the second quarter of 2020.[30] The second leading tablet vendor, Samsung, accounted for only 18.7%.[31]

177. Apple has also been able to maintain its pricing power in the sale of tablets. Whereas the average global selling price of tablets in 2016 was $285, increasing to an average selling price of $357 by the end of the second quarter of 2020, Apple's iPads maintained an average selling price of over $200 higher, with an average selling price of $528 (in 2016) and $575 (end of the second quarter of 2020).[32]

C. Information Costs and Other Market Inefficiencies in the iOS App Distribution and iOS In-App Payment Processing Markets.

178. There is a further reason that competition at the mobile device level does not constrain Apple's power in the iOS App Distribution and iOS In-App Payment Processing Markets, which is that consumers cannot adequately account for Apple's downstream anti-competitive conduct through their mobile device purchasing behavior.

179. Consumers are rationally ignorant of Apple's anti-competitive conduct described above in Parts I and II. As a threshold matter, the vast majority of

---

[29] Statista Research Department, "Revenue of Apple from iPad Sales Worldwide From 3rd Quarter 2010 to 3rd Quarter 2020", *Statista* (Aug. 7, 2020), online at https://www.statista.com/statistics/269914/apples-global-revenue-from-ipad-sales-by-quarter/#:~:text=Apple's%20global%20revenue%20from%20iPad%20sales%202010%2D2020&text=In%20the%20third%20quarter%20of,the%20third%20quarter%20of%202019 (last accessed Aug. 11, 2020).

[30] "Worldwide Tablet PC Market Q2 2020", *Canalys* (Aug. 3, 2020), online at https://www.canalys.com/newsroom/canalys-worldwide-tablet-pc-market-Q2-2020 (last accessed Aug. 11, 2020).

[31] *Id.*

[32] IDC, "IDC Quarterly Personal Computing Device Tracker" (Aug. 7, 2020).

mobile device consumers have no reason to inquire, and therefore do not know, about Apple's anti-competitive contractual restraints and policies; it would not even occur to them to research or ask about Apple's app distribution or in-app payment processing policies, which touch them only indirectly. Because many consumers do not know of Apple's anti-competitive conduct, they cannot take into it account when deciding which smartphone or tablet to purchase. It should also be noted that when purchasing iPhones and iPads, consumers do not contractually agree to permit Apple to engage in the anti-competitive conduct described above in Parts I and II.

180. More fundamentally, even those consumers that do know of Apple's anti-competitive conduct in the iOS App Distribution and iOS In-App Payment Processing Markets do not account for the costs of that conduct when deciding which mobile device to purchase for a number of reasons.

181. *First*, the complexity of device pricing obscures the impact of Apple's anti-competitive conduct. Consumers consider many features when deciding which smartphone or tablet to purchase, including design, brand, processing power, battery life, functionality, cellular plan and provider coverage, etc. These features are likely to play a substantially larger role in a consumer's decision as to which smartphone or tablet to purchase than Apple's anti-competitive conduct in the iOS App Distribution and iOS In-App Payment Processing Markets (if it plays a role at all), particularly given that each individual app and in-app purchase is a relatively small monetary cost when compared to the price of the device. For example, Apple's iPhone 11 currently retails starting at $699, while the two new flagship phones, iPhone 11 Pro and Pro Max, retail starting at $999 and $1,099, respectively.[33] In 2019, the median price of paid apps on the App Store

[33] Dami Lee, "The iPhone 11, Pro, and Pro Max will cost $699, $999, and $1,099, respectively", *The Verge* (Sep. 10, 2019), https://www.theverge.com/2019/9/10/20848182/new-iphone-11-price-cost-announcement-699-apple.

amounted to only $1.99,[34] and U.S. iPhone users spent an average $100 on apps (including in-app purchases) for the year.[35] Apple's 30% tax on this amount represents only 4.2% of the iPhone 11's retail price. Given the small cost of apps relative to the price of Apple's iPhones, Apple's tax is an effective means by which Apple may exercise its monopoly power in the iOS App Distribution and iOS In-App Payment Processing Markets without affecting mobile device purchases.

182. *Second*, consumers are unable to determine the "lifecycle price" of devices—*i.e.*, to accurately assess at the point of purchase how much they will end up spending in total (including on the device and all apps and in-app purchases) for the duration of their ownership of the device. Consumers cannot know in advance of purchasing a device all of the apps or in-app content that they may want to purchase during the usable lifetime of the device. Consumers' circumstances may change. Consumers may develop new interests. They may learn about new apps or in-app content that becomes available only after purchasing a device. According to Apple, "the App Store is the best place to discover new apps that let you pursue your passions in ways you never thought possible."[36] New apps and in-app content will continue to be developed and marketed after a consumer purchases a smartphone or tablet. All of these factors may influence the amount of consumers' app and in-app purchases. Because they cannot know or predict all such factors when purchasing mobile devices, consumers are unable to calculate the lifecycle prices of the devices. This prevents consumers from effectively taking Apple's anti-competitive conduct in the iOS App Distribution and iOS In-App Payment Processing Markets into account when making mobile device purchasing decisions.

---

[34] J. Clement, "Average Price of Paid Android and iOS Apps 2018", *Statista* (Mar. 22, 2019), online at https://www.statista.com/statistics/262387/average-price-of-android-ipad-and-iphone-apps/ (last accessed Aug. 3, 2020).

[35] Randy Nelson, "U.S. iPhone Users Spent an Average of $100 on Apps in 2019, Up 27% From 2018", *Sensor Tower* (Mar. 25, 2020), online at https://sensortower.com/blog/revenue-per-iphone-2019.

[36] Apple, *App Store*, online at https://www.apple.com/ios/app-store/ (last accessed July 27, 2020).

183. *Third*, Apple's anti-competitive conduct in the iOS App Distribution and iOS In-App Payment Processing Markets does not incentivize consumers to purchase a non-iOS mobile device because Google engages in similar anti-competitive conduct. As noted, nearly 100% of all mobile devices run either Apple's iOS or Google's Android OS. Further, more than 90% of app downloads on Android OS devices occur through the Google Play Store—Google's app store. Like Apple, Google uses its market power over the Android operating system, and similar anti-competitive practices, to stifle competition for the distribution of apps on Android, to require that developers use its payment processing system for in-app purchases of in-app content, and to charge a similar exorbitant 30% tax. Thus, to the extent that consumers even attempt to lifecycle price when purchasing mobile devices, or want to look for an app store that doesn't charge exorbitant fees, Apple's anti-competitive conduct described herein would not cause consumers to favor Android devices.

COUNT 1: Sherman Act § 2

(Unlawful Monopoly Maintenance in the iOS App Distribution Market)

184. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

185. Apple's conduct violates Section 2 of the Sherman Act, which prohibits the "monopoliz[ation of] any part of the trade or commerce among the several States, or with foreign nations". 15 U.S.C. § 2.

186. The iOS App Distribution Market is a valid antitrust market.

187. Apple holds monopoly power in the iOS App Distribution Market.

188. Apple unlawfully maintains its monopoly power in the iOS App Distribution Market through the anti-competitive acts described herein, including by imposing technical and contractual restrictions on iOS, which prevents the distribution of iOS apps through means other than the App Store and prevents developers from distributing competing app stores to iOS users.

189. Apple's conduct affects a substantial volume of interstate as well as foreign commerce.

190. Apple's conduct has substantial anti-competitive effects, including increased prices and costs, reduced innovation and quality of service, and lowered output.

191. As an app distributor and as an app developer, Epic has been harmed by Apple's anti-competitive conduct in a manner that the antitrust laws were intended to prevent. Epic has suffered and continues to suffer harm and irreparable injury, and such harm and injury will not abate until an injunction ending Apple's anti-competitive conduct issues.

192. To prevent these ongoing harms, the Court should enjoin the anti-competitive conduct complained of herein.

COUNT 2: Sherman Act § 2

(Denial of Essential Facility in the iOS App Distribution Market)

193. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

194. Apple's conduct violates Section 2 of the Sherman Act, which prohibits the "monopoliz[ation of] any part of the trade or commerce among the several States, or with foreign nations". 15 U.S.C. § 2.

195. The iOS App Distribution Market is a valid antitrust market.

196. Apple holds monopoly power in the iOS App Distribution Market.

197. Apple unlawfully maintains its monopoly power in the iOS App Distribution Market through its unlawful denial to Epic and other app distributors of an essential facility—access to iOS—which prevents them from competing in the iOS App Distribution Market.

198. Apple controls iOS, which is essential to effective competition in the iOS App Distribution Market.

199. App distributors are unable to reasonably or practically duplicate Apple's iOS.

200. It is technically feasible for Apple to provide access to iOS to Epic and other app distributors, and it would not interfere with or significantly inhibit Apple's ability to conduct its business.

201. Apple's denial of access to iOS has no legitimate business purpose, and serves only to assist Apple in maintaining its unlawful monopoly position in the iOS App Distribution Market.

202. Through its denial of its essential facility, Apple maintains its monopoly power in the iOS App Distribution Market.

203. Apple's conduct affects a substantial volume of interstate as well as foreign commerce.

204. Apple's conduct has substantial anti-competitive effects, including increased prices and costs, reduced innovation and quality of service, and lowered output.

205. As an app distributor and as an app developer, Epic has been harmed by Apple's anti-competitive conduct in a manner that the antitrust laws were intended to prevent. Epic has suffered and continues to suffer harm and irreparable injury, and such harm and injury will not abate until an injunction ending Apple's anti-competitive conduct issues.

206. To prevent these ongoing harms, the Court should enjoin the anti-competitive conduct complained of herein.

COUNT 3: Sherman Act § 1

(Unreasonable Restraints of Trade in the iOS App Distribution Market)

207. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

208. Apple's conduct violates Section 1 of the Sherman Act, which prohibits "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations". 15 U.S.C. § 1.

209. The iOS App Distribution Market is a valid antitrust market.

210. To reach iOS users, Apple forces developers to agree to Apple's unlawful terms contained in its Developer Agreement and to comply with Apple's App Store Review Guidelines, including the requirement iOS developers distribute their apps through the App Store. These contractual provision unlawfully foreclose the iOS App Distribution Market to competitors and maintain Apple's monopoly.

211. The challenged provisions of the Developer Agreement and the terms of Apple's App Store Review Guidelines unreasonably restrain competition in the iOS App Distribution Market and serve no legitimate or pro-competitive purpose that could justify their anti-competitive effects.

212. Apple's conduct and unlawful contractual restraints affect a substantial volume of interstate as well as foreign commerce.

213. Apple's conduct has substantial anti-competitive effects, including increased prices to users and increased costs to developers, reduced innovation, and reduced quality of service and lowered output.

214. Apple's conduct has caused Epic, as an app distributor, to suffer injury to its business by foreclosing Epic from competing in the iOS App Distribution Market. Epic is also harmed as an app developer because it has no choices for distributing its apps to iOS device users other than the App Store and therefore suffers the anti-competitive effects felt by all app developers that are described above. Epic has been and continues to be directly harmed by Apple's anti-competitive conduct in a manner that the antitrust laws were intended to prevent. Epic has suffered and continues to suffer harm and irreparable injury, and such harm and injury will not abate until an injunction ending Apple's anti-competitive conduct issues.

215. To prevent these ongoing harms, the Court should enjoin the anti-competitive conduct complained of herein.

COUNT 4: Sherman Act § 2

(Unlawful Monopoly Maintenance in the iOS In-App Payment Processing Market)

216. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

217. Apple's conduct violates Section 2 of the Sherman Act, which prohibits the "monopoliz[ation of] any part of the trade or commerce among the several States, or with foreign nations". 15 U.S.C. § 2.

218. The iOS In-App Payment Processing Market is a valid antitrust market. In the alternative, the iOS Games Payment Processing Market is a valid antitrust market.

219. Apple has monopoly power in the iOS In-App Payment Processing Market and, in the alternative, in the iOS Games Payment Processing Market.

220. Apple has unlawfully maintained its monopoly in these markets through the anti-competitive acts alleged herein, including by forcing, through its contractual terms and unlawful policies, iOS app developers that sell in-app content to exclusively use Apple's In-App Purchase, and preventing and discouraging app developers from developing or integrating alternative payment processing solutions.

221. Apple's conduct affects a substantial volume of interstate as well as foreign commerce.

222. Apple's conduct has substantial anti-competitive effects, including increased prices and costs, reduced innovation, and quality of service and lowered output.

223. As an app developer and as the developer of a competing in-app payment processing tool, Epic has been harmed by Apple's anti-competitive conduct in a manner that the antitrust laws were intended to prevent. Epic has suffered and continues to suffer harm and irreparable injury, and such harm and injury will not abate until an injunction ending Apple's anti-competitive conduct issues.

224. To prevent these ongoing harms, the Court should enjoin the anti-competitive conduct complained of herein.

COUNT 5: Sherman Act § 1

(Unreasonable Restraints of Trade in the iOS In-App Payment Processing Market)

225. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

226. Apple's conduct violates Section 1 of the Sherman Act, which prohibits "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations". 15 U.S.C. § 1.

227. To reach iOS app users, Apple forces developers to agree to Apple's unlawful terms contained in its Developer Agreement, including that they use Apple's In-App Purchase for in-app purchases of in-app content to the exclusion of any alternative solution or third-party payment processor. Further, Section 3.1.3 of Apple's App Store Review Guidelines unlawfully prohibits developers from "directly or indirectly target[ing] iOS users to use a purchasing method other than in-app purchase".

228. Apple's challenged contractual provisions and policy guidelines serve no legitimate or pro-competitive purpose and unreasonably restrain competition in the iOS In-App Payment Processing Market and, in the alternative, in the iOS Games Payment Processing Market.

229. Apple's conduct and unlawful contractual restraints affect a substantial volume of interstate as well as foreign commerce.

230. Apple's conduct has substantial anti-competitive effects, including increased prices to users and increased costs to developers, reduced innovation, and reduced quality of service and lowered output.

231. Apple's conduct has foreclosed Epic from participating in the iOS In-App Payment Processing Market and, in the alternative, in the iOS Games Payment Processing Market. Epic has also been harmed in its capacity as an app developer by being deprived of a choice of in-app payment processing tools, denied the benefits of innovation in in-app payment processing, and forced to pay a supra-competitive rate for

in-app payment processing. Epic has been harmed by Apple's anti-competitive conduct in a manner that the antitrust laws were intended to prevent. Epic has suffered and continues to suffer harm and irreparable injury, and such harm and injury will not abate until an injunction ending Apple's anti-competitive conduct issues.

232. To prevent these ongoing harms, the Court should enjoin the anti-competitive conduct complained of herein.

COUNT 6: Sherman Act § 1

(Tying the App Store in the iOS App Distribution Market to In-App Purchase in the iOS In-App Payment Processing Market)

233. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

234. Apple's conduct violates Section 1 of the Sherman Act, which prohibits "[e]very contract, combination in the form of trust or otherwise, or conspiracy, in restraint of trade or commerce among the several States, or with foreign nations". 15 U.S.C. § 1.

235. Through its Developer Agreement with app developers and its App Store Review Guidelines, Apple has unlawfully tied its in-app payment processor, In-App Purchase, to the use of its App Store.

236. Apple has sufficient economic power in the tying market, the iOS App Distribution Market, because the App Store is the sole means by which apps may be distributed to consumers in that market.

237. Apple is able to unlawfully condition access to the App Store on the developer's use of a second product—In-App Purchase—for in-app sales of in-app content. Through its Developer Agreement and unlawful policies, Apple expressly conditions the use of its App Store on the use of its In-App Purchase to the exclusion of alternative solutions in a *per se* unlawful tying arrangement.

238. The tying product, Apple's App Store, is distinct from the tied product, Apple's In-App Purchase, because app developers such as Epic have alternative

in-app payment processing options and would prefer to choose among them independently of how the developer's iOS apps are distributed. In other words, app developers are coerced into using In-App Purchase by virtue of wanting to use the App Store. Apple's unlawful tying arrangement thus ties two separate products that are in separate markets and coerces Epic and other developers to rely on both of Apple's products.

239. Apple's conduct has foreclosed, and continues to foreclose, competition in the iOS In-App Payment Processing Market and, in the alternative, in the iOS Games Payment Processing Market, affecting a substantial volume of commerce in these markets.

240. Apple has thus engaged in a *per se* illegal tying arrangement and the Court does not need to engage in a detailed assessment of the anti-competitive effects of Apple's conduct or its purported justifications.

241. In the alternative only, even if Apple's conduct does not constitute a *per se* illegal tie, an analysis of Apple's tying arrangement would demonstrate that this arrangement violates the rule of reason and is illegal by coercing developers into using its In-App Purchase product.

242. Apple's conduct harms Epic which, as a direct result of Apple's anti-competitive conduct, is paying supra-competitive fees on in-app purchases processed through Apple's payment processor and has forgone revenue it would be able to generate if its own in-app payment processor were not unreasonably restricted from the market.

243. As an app developer that consumes in-app payment processing services and as the developer of a competing in-app payment processing tool, Epic has a direct financial interest in the iOS In-App Payment Processing Market and, in the alternative, in the iOS Games Payment Processing Market, and has been foreclosed from competing with Apple directly as a result of Apple's unlawful tie.

244. Epic has been harmed by Apple's anti-competitive conduct in a manner that the antitrust laws were intended to prevent. Epic has suffered and continues

to suffer harm and irreparable injury, and such harm and injury will not abate until an injunction ending Apple's anti-competitive conduct issues.

245. To prevent these ongoing harms, the Court should enjoin the anti-competitive conduct complained of herein.

COUNT 7: California Cartwright Act

(Unreasonable Restraints of Trade in the iOS App Distribution Market)

246. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

247. Apple's acts and practices detailed above violate the Cartwright Act, Cal. Bus. & Prof. Code § 16700 *et seq.*, which prohibits, *inter alia*, the combination of resources by two or more persons to restrain trade or commerce or to prevent market competition. *See* §§ 16720, 16726.

248. Under the Cartwright Act, a "combination" is formed when the anti-competitive conduct of a single firm coerces other market participants to involuntarily adhere to the anti-competitive scheme.

249. The iOS App Distribution Market is a valid antitrust market.

250. Apple has monopoly power in the iOS App Distribution Market.

251. Apple forces developers to agree to Apple's unlawful terms contained in its Developer Agreement, including that iOS developers distribute their apps through the App Store. Section 3.2(g) of the Developer Agreement contains the unlawful requirement that developers distribute their apps through the App Store. Apple also conditions app distributors' access to iOS on their agreement not to distribute third-party app stores. Section 3.3.2(b) of the Developer Agreement prohibits "Application[s]" that "create a store or storefront for other code or applications". These provisions unreasonably restrain competition in the iOS App Distribution Market.

252. These challenged provisions have no legitimate or pro-competitive purpose or effect, and unreasonably restrain competition in the iOS App Distribution Market.

253. Apple's conduct and practices have substantial anti-competitive effects, including increased prices and costs, reduced innovation, poorer quality of customer service, and lowered output.

254. Apple's conduct harms Epic which, as a direct result of Apple's anti-competitive conduct, has been unreasonably restricted in its ability to distribute its iOS applications, including *Fortnite*, and to market a competing app store to the App Store.

255. It is appropriate to bring this action under the Cartwright Act because many of the illegal agreements were made in California and purport to be governed by California law, many affected consumers and developers reside in California, Apple has its principal place of business in California, and overt acts in furtherance of Apple's anti-competitive scheme took place in California.

256. Epic has suffered and continues to suffer harm, and such harm will not abate until an injunction ending Apple's anti-competitive conduct issues. To prevent these ongoing harms, the Court should enjoin the anti-competitive conduct complained of herein.

COUNT 8: California Cartwright Act
(Unreasonable Restraints of Trade in the iOS In-App Payment Processing Market)

257. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

258. Apple's acts and practices detailed above violate the Cartwright Act, Cal. Bus. & Prof. Code § 16700 *et seq.*, which prohibits, *inter alia*, the combination of resources by two or more persons to restrain trade or commerce or to prevent market competition. *See* §§ 16720, 16726.

259. Under the Cartwright Act, a "combination" is formed when the anti-competitive conduct of a single firm coerces other market participants to involuntarily adhere to the anti-competitive scheme.

260. The iOS In-App Payment Processing Market and, in the alternative, the iOS Games Payment Processing Market, are valid antitrust markets.

261. Apple has monopoly power in the iOS In-App Payment Processing Market and, in the alternative, in the iOS Games Payment Processing Market.

262. Apple conditions distribution through the App Store on entering into the Developer Agreement described above, including the contractual and policy restrictions contained therein and in the App Store Review Guidelines. Through certain provisions in these agreements, Apple forces app developers to submit to conditions that unreasonably restrain competition in the iOS In-App Payment Processing Market and, in the alternative, the iOS Games Payment Processing Market.

263. Section 3.1.1 of the App Store Review Guidelines provide that "if you [the developer] want to unlock features or functionality within your app, (by way of example: subscriptions, in-game currencies, game levels, access to premium content, or unlocking a full version), you *must use in-app purchase*. Apps *may not use their own mechanisms to unlock content or functionality* . . . ." (emphases added). Finally, Section 3.1.3 of the guidelines provides that developers may not "directly or indirectly target iOS users to use a purchasing method *other than [Apple's] in-app purchase*, and general communications [to users] about other purchasing methods [must not be] *designed to discourage use of [Apple's] in-app purchase*". (emphases added).

264. These provisions have no legitimate or pro-competitive purpose or effect, and unreasonably restrain competition in the iOS In-App Payment Processing Market and, in the alternative, in the iOS Games Payment Processing Market.

265. Apple's conduct and practices have substantial anti-competitive effects, including increased prices and costs, reduced innovation, poorer quality of customer service, and lowered output.

266. Apple's conduct harms Epic which, as a direct result of Apple's anti-competitive conduct, has been unreasonably restricted in its ability to distribute and use its own in-app payment processor and forced to pay Apple's supra-competitive fees.

267. It is appropriate to bring this action under the Cartwright Act because many of the illegal agreements were made in California and purport to be governed by

California law, many affected consumers and developers reside in California, Apple has its principal place of business in California, and overt acts in furtherance of Apple's anti-competitive scheme took place in California.

268. Epic has suffered and continues to suffer harm and irreparable injury, and such harm and injury will not abate until an injunction ending Apple's anti-competitive conduct issues. To prevent these ongoing harms, the Court should enjoin the anti-competitive conduct complained of herein.

COUNT 9: California Cartwright Act

(Tying the App Store in the iOS App Distribution Market to In-App Purchase in the iOS In-App Payment Processing Market)

269. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

270. Apple's acts and practices detailed above violate the Cartwright Act, Cal. Bus. & Prof. Code § 16700 *et seq.*, which prohibits, *inter alia*, the combination of resources by two or more persons to restrain trade or commerce, or to prevent market competition. *See* §§ 16720, 16726.

271. Under the Cartwright Act, a "combination" is formed when the anti-competitive conduct of a single firm coerces other market participants to involuntarily adhere to the anti-competitive scheme.

272. The Cartwright Act also makes it "unlawful for any person to lease or make a sale or contract for the sale of goods, merchandise, machinery, supplies, commodities for use within the State, or to fix a price charged therefor, or discount from, or rebate upon, such price, on the condition, agreement or understanding that the lessee or purchaser thereof shall not use or deal in the goods, merchandise, machinery, supplies, commodities, or services of a competitor or competitors of the lessor or seller, where the effect of such lease, sale, or contract for sale or such condition, agreement or understanding may be to substantially lessen competition or tend to create a monopoly in any line of trade or commerce in any section of the State." § 16727.

273. As detailed above, Apple has unlawfully tied its in-app payment processor, In-App Purchase, to the App Store through its Developer Agreement and App Store Review Guidelines.

274. Apple has sufficient economic power in the tying market, the iOS App Distribution Market, to affect competition in the tied market, the iOS In-App Payment Processing Market and, in the alternative, the iOS Game Payment Processing Market. With Apple's unlawful conditions and policies, Apple ensures that the App Store is the only distribution channel for developers to reach iOS app users, giving Apple overwhelming monopoly power in the iOS App Distribution Market. Apple's power is further evidenced by its ability to extract supra-competitive taxes on the sale of apps through the App Store.

275. The availability of the App Store for app distribution is conditioned on the app developer accepting a second product, Apple's in-app payment processing services. Apple's foreclosure of alternative app distribution channels coerces developers like Epic to use Apple's in-app payment processing services, which Apple has expressly made a condition of reaching Apple iOS through its App Store. In other words, app developers are coerced into using In-App Purchase by virtue of wanting to use the App Store.

276. The tying product, iOS app distribution, is separate and distinct from the tied product, iOS in-app payment processing, because app developers such as Epic have alternative in-app payment processing options and would prefer to choose among them independently of how an iOS app is distributed. Apple's unlawful tying arrangement thus ties two separate products that are in separate markets.

277. Apple's conduct forecloses competition in the iOS In-App Payment Processing Market and, in the alternative, in the iOS Games Payment Processing Market, affecting a substantial volume of commerce in this market.

278. Apple has thus engaged in a *per se* illegal tying arrangement and the Court does not need to engage in a detailed assessment of the anti-competitive effects of Apple's conduct or its purported justifications.

279. Even if Apple's conduct does not form a *per se* illegal tie, an assessment of the tying arrangement would demonstrate that it is unreasonable under the Cartwright Act, and therefore, illegal.

280. Apple's acts and practices detailed above unreasonably restrain competition in the iOS In-App Payment Processing Market and, in the alternative, in the iOS Games Payment Processing Market.

281. Apple's conduct harms Epic which, as a direct result of Apple's anti-competitive conduct, is paying a supra-competitive commission rate on in-app purchases processed through Apple's payment processor and has forgone commission revenue it would be able to generate if its own in-app payment processor were not unreasonably restricted from the market.

282. As an app developer which consumes in-app payment processing services and as the developer of a competing in-app payment processing tool, Epic has been harmed by Apple's anti-competitive conduct in a manner that the antitrust laws were intended to prevent.

283. It is appropriate to bring this action under the Cartwright Act because many of the illegal agreements were made in California and purport to be governed by California law, many affected consumers and developers reside in California, Apple has its principal place of business in California, and overt acts in furtherance of Apple's anti-competitive scheme took place in California.

284. Epic has suffered and continues to suffer harm, and such harm will not abate until an injunction ending Apple's anti-competitive conduct issues. To prevent these ongoing harms, the Court should enjoin the anti-competitive conduct complained of herein.

COUNT 10: California Unfair Competition Law

285. Epic restates, re-alleges, and incorporates by reference each of the allegations set forth in the rest of this Complaint as if fully set forth herein.

286. Apple's conduct, as described above, violates California's Unfair Competition Law, Cal. Bus. & Prof. Code §§ 17200, *et seq.*, which prohibits any unlawful, unfair, or fraudulent business act or practice.

287. Epic has standing to bring this claim because it has suffered injury in fact and lost money as a result of Apple's unfair competition. Specifically, it develops and distributes apps for iOS, has developed a payment processor for in-app purchases, and Apple's conduct has unreasonably restricted Epic's ability to fairly compete in the relevant markets with these products.

288. Apple's conduct violates the Sherman Act and the Cartwright Act, and thus constitutes unlawful conduct under § 17200.

289. Apple's conduct is also "unfair" within the meaning of the Unfair Competition Law.

290. Apple's conduct harms Epic which, as a direct result of Apple's anti-competitive conduct, is unreasonably prevented from freely distributing mobile apps or its in-app payment processing tool, and forfeits a higher commission rate on the in-app purchases than it would pay absent Apple's conduct.

291. Epic seeks injunctive relief under the Unfair Competition Law.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff Epic respectfully requests that the Court enter judgment in favor of Epic and against Defendant Apple:

A. Issuing an injunction prohibiting Apple's anti-competitive conduct and mandating that Apple take all necessary steps to cease unlawful conduct and to restore competition;

B. Awarding a declaration that the contractual and policy restraints complained of herein are unlawful and unenforceable;

C. Awarding any other equitable relief necessary to prevent and remedy Apple's anti-competitive conduct; and

D. Granting such other and further relief as the Court deems just and proper.

Dated: August 13, 2020

Respectfully submitted,

By: /s/ Paul J. Riehle

Paul J. Riehle (SBN 115199)
paul.riehle@faegredrinker.com
FAEGRE DRINKER BIDDLE & REATH LLP
Four Embarcadero Center
San Francisco, California 94111
Telephone: (415) 591-7500
Facsimile: (415) 591-7510

CRAVATH, SWAINE & MOORE LLP

Christine A. Varney (*pro hac vice pending*)
cvarney@cravath.com
Katherine B. Forrest (*pro hac vice pending*)
kforrest@cravath.com
Gary A. Bornstein (*pro hac vice pending*)
gbornstein@cravath.com
Yonatan Even (*pro hac vice pending*)
yeven@cravath.com
M. Brent Byars (*pro hac vice pending)*
mbyars@cravath.com

825 Eighth Avenue
New York, New York 10019
Telephone: (212) 474-1000
Facsimile: (212) 474-3700

Exhibit A

PLEASE READ THE FOLLOWING APPLE DEVELOPER PROGRAM LICENSE AGREEMENT TERMS AND CONDITIONS CAREFULLY BEFORE DOWNLOADING OR USING THE APPLE SOFTWARE OR APPLE SERVICES. THESE TERMS AND CONDITIONS CONSTITUTE A LEGAL AGREEMENT BETWEEN YOU AND APPLE.

Apple Developer Program License Agreement

Purpose

You would like to use the Apple Software (as defined below) to develop one or more Applications (as defined below) for Apple-branded products. Apple is willing to grant You a limited license to use the Apple Software and Services provided to You under this Program to develop and test Your Applications on the terms and conditions set forth in this Agreement.

Applications developed under this Agreement for iOS Products, Apple Watch, or Apple TV can be distributed in four ways: (1) through the App Store, if selected by Apple, (2) through the Custom App Distribution, if selected by Apple, (3) on a limited basis for use on Registered Devices (as defined below), and (4) for beta testing through TestFlight. Applications developed for macOS can be distributed through the App Store, if selected by Apple, or separately distributed under this Agreement.

Applications that meet Apple's Documentation and Program Requirements may be submitted for consideration by Apple for distribution via the App Store, Custom App Distribution, or for beta testing through TestFlight. If submitted by You and selected by Apple, Your Applications will be digitally signed by Apple and distributed, as applicable. Distribution of free (no charge) Applications (including those that use the In-App Purchase API for the delivery of free content) via the App Store or Custom App Distribution will be subject to the distribution terms contained in Schedule 1 to this Agreement. If You would like to distribute Applications for which You will charge a fee or would like to use the In-App Purchase API for the delivery of fee-based content, You must enter into a separate agreement with Apple ("Schedule 2"). If You would like to distribute paid Applications via Custom App Distribution, You must enter into a separate agreement with Apple ("Schedule 3"). You may also create Passes (as defined below) for use on Apple-branded products running iOS or watchOS under this Agreement and distribute such Passes for use by Wallet.

1. Accepting this Agreement; Definitions

1.1 Acceptance

In order to use the Apple Software and Services, You must first accept this Agreement. If You do not or cannot accept this Agreement, You are not permitted to use the Apple Software or Services. Do not download or use the Apple Software or Services in that case. You accept and agree to the terms of this Agreement on Your own behalf and/or on behalf of Your company, organization, educational institution, or agency, instrumentality, or department of the federal government as its authorized legal representative, by doing either of the following:
(a) checking the box displayed at the end of this Agreement if You are reading this on an Apple website; or
(b) clicking an "Agree" or similar button, where this option is provided by Apple.

1.2 Definitions

Whenever capitalized in this Agreement:

"**Ad Network APIs**" means the Documented APIs that provide a way to validate the successful conversion of advertising campaigns on supported Apple-branded products using a combination of cryptographic signatures and a registration process with Apple.

"**Ad Support APIs**" means the Documented APIs that provide the Advertising Identifier and Advertising Preference.

"**Advertising Identifier**" means a unique, non-personal, non-permanent identifier provided through the Ad Support APIs that are associated with a particular Apple-branded device and are to be used solely for advertising purposes, unless otherwise expressly approved by Apple in writing.

"**Advertising Preference**" means the Apple setting that enables an end-user to set an ad tracking preference.

"**Agreement**" means this Apple Developer Program License Agreement, including any attachments, Schedule 1 and any exhibits thereto which are hereby incorporated by this reference. For clarity, this Agreement supersedes the iOS Developer Program License Agreement (including any attachments, Schedule 1 and any exhibits thereto), the Safari Extensions Digital Signing Agreement, the Safari Extensions Gallery Submission Agreement, and the Mac Developer Program License Agreement.

"**App Store**" means an electronic store and its storefronts branded, owned, and/or controlled by Apple, or an Apple Subsidiary or other affiliate of Apple, through which Licensed Applications may be acquired.

"**App Store Connect**" means Apple's proprietary online content management tool for Applications.

"**Apple**" means Apple Inc., a California corporation with its principal place of business at One Apple Park Way, Cupertino, California 95014, U.S.A.

"**Apple Certificates**" means the Apple-issued digital certificates provided to You by Apple under the Program.

"**Apple Maps Service**" means the mapping platform and Map Data provided by Apple via the MapKit API for use by You only in connection with Your Applications, or the mapping platform and Map Data provided by Apple via MapKit JS and related tools for capturing map content (e.g., MapSnapshotter) for use by You only in connection with Your Applications, websites, or web applications.

"**Apple Pay APIs**" means the Documented APIs that enable end-users to send payment information they have stored on a supported Apple-branded product to an Application to be used in payment transactions made by or through the Application, and includes other payment-related functionality as described in the Documentation.

"**Apple Pay Payload**" means a customer data package passed through the Apple Software and Apple Pay APIs as part of a payment transaction (e.g., name, email, billing address, shipping address, and device account number).

"**Apple Push Notification Service**" or "**APN**" means the Apple Push Notification service that Apple may provide to You to enable You to transmit Push Notifications to Your Application or for use as otherwise permitted herein.

"**APN API**" means the Documented API that enables You to use the APN to deliver a Push Notification to Your Application or for use as otherwise permitted herein.

"**Apple Services**" or "**Services**" means the developer services that Apple may provide or make available through the Apple Software or as part of the Program for use with Your Covered

Products or development, including any Updates thereto (if any) that may be provided to You by Apple under the Program.

"**Apple Software**" means Apple SDKs, iOS, watchOS, tvOS, iPadOS, and/or macOS, the Provisioning Profiles, FPS SDK, FPS Deployment Package, and any other software that Apple provides to You under the Program, including any Updates thereto (if any) that may be provided to You by Apple under the Program.

"**Apple SDKs**" means the Apple-proprietary Software Development Kits (SDKs) provided hereunder, including but not limited to header files, APIs, libraries, simulators, and software (source code and object code) labeled as part of iOS, watchOS, tvOS, iPadOS, or Mac SDK and included in the Xcode Developer Tools package for purposes of targeting Apple-branded products running iOS, watchOS, tvOS, iPadOS, and/or macOS, respectively.

"**Apple Subsidiary**" means a corporation at least fifty percent (50%) of whose outstanding shares or securities (representing the right to vote for the election of directors or other managing authority) are owned or controlled, directly or indirectly, by Apple, and that is involved in the operation of or otherwise affiliated with the App Store, Custom App Distribution, TestFlight, and as otherwise referenced herein (e.g., Attachment 4).

"**Apple TV**" means an Apple-branded product that runs the tvOS.

"**Apple Watch**" means an Apple-branded product that runs the watchOS.

"**Application**" means one or more software programs (including extensions, media, and Libraries that are enclosed in a single software bundle) developed by You in compliance with the Documentation and the Program Requirements, for distribution under Your own trademark or brand, and for specific use with an Apple-branded product running iOS, iPadOS, watchOS, tvOS, or macOS, as applicable, including bug fixes, updates, upgrades, modifications, enhancements, supplements to, revisions, new releases and new versions of such software programs.

"**Authorized Developers**" means Your employees and contractors, members of Your organization or, if You are an educational institution, Your faculty and staff who (a) each have an active and valid Apple Developer account with Apple, (b) have a demonstrable need to know or use the Apple Software in order to develop and test Covered Products, and (c) to the extent such individuals will have access to Apple Confidential Information, each have written and binding agreements with You to protect the unauthorized use and disclosure of such Apple Confidential Information.

"**Authorized Test Units**" means Apple-branded hardware units owned or controlled by You that have been designated by You for Your own testing and development purposes under this Program, and if You permit, Apple-branded hardware units owned or controlled by Your Authorized Developers so long as such units are used for testing and development purposes on Your behalf and only as permitted hereunder.

"**Beta Testers**" means end-users whom You have invited to sign up for TestFlight in order to test pre-release versions of Your Application and who have accepted the terms and conditions of the TestFlight Application.

"**ClassKit APIs**" means the Documented APIs that enable You to send student progress data for use in a school-managed environment.

"**CloudKit APIs**" means the Documented APIs that enable Your Applications, Web Software, and/or Your end-users (if You permit them) to read, write, query and/or retrieve structured data from public and/or private containers in iCloud.

"**Configuration Profile(s)**" means an XML file that allows You to distribute configuration information (e.g., VPN or Wi-Fi settings) and restrictions on device features (e.g., disabling the camera) to compatible Apple-branded products through Apple Configurator or other similar Apple-branded software tools, email, a webpage, or over-the-air deployment, or via Mobile Device Management (MDM). For the sake of clarity, unless otherwise expressly permitted by Apple in writing, MDM is available only for enterprise use and is separately licensed for under the Apple Developer Enterprise Program License Agreement.

"**Corresponding Products**" means web-based or other versions of Your software applications that have the same title and substantially equivalent features and functionality as Your Licensed Application (e.g., feature parity).

"**Covered Products**" means Your Applications, Libraries, Passes, Safari Extensions, Safari Push Notifications, and/or FPS implementations developed under this Agreement.

"**Custom App Distribution**" means the store or storefront functionality that enables users to obtain Licensed Applications through the use of Apple Business Manager, Apple School Manager, or as otherwise permitted by Apple.

"**DeviceCheck APIs**" means the set of APIs, including server-side APIs, that enable You to set and query two bits of data associated with a device and the date on which such bits were last updated.

"**DeviceCheck Data**" means the data stored and returned through the DeviceCheck APIs.

"**Documentation**" means any technical or other specifications or documentation that Apple may provide to You for use in connection with the Apple Software, Apple Services, Apple Certificates, or otherwise as part of the Program.

"**Documented API(s)**" means the Application Programming Interface(s) documented by Apple in published Apple Documentation and which are contained in the Apple Software.

"**Face Data**" means information related to human faces (e.g., face mesh data, facial map data, face modeling data, facial coordinates or facial landmark data, including data from an uploaded photo) that is obtained from a user's device and/or through the use of the Apple Software (e.g., through ARKit, the Camera APIs, or the Photo APIs), or that is provided by a user in or through an Application (e.g., uploads for a facial analysis service).

"**FPS**" or "**FairPlay Streaming**" means Apple's FairPlay Streaming Server key delivery mechanism as described in the FPS SDK.

"**FPS Deployment Package**" means the D Function specification for commercial deployment of FPS, the D Function reference implementation, FPS sample code, and set of unique production keys specifically for use by You with an FPS implementation, if provided by Apple to You.

"**FPS SDK**" means the FPS specification, FPS server reference implementation, FPS sample code, and FPS development keys, as provided by Apple to You.

"**FOSS**" (Free and Open Source Software) means any software that is subject to terms that, as a condition of use, copying, modification or redistribution, require such software and/or derivative works thereof to be disclosed or distributed in source code form, to be licensed for the purpose of making derivative works, or to be redistributed free of charge, including without limitation software distributed under the GNU General Public License or GNU Lesser/Library GPL.

"**Game Center**" means the gaming community service and related APIs provided by Apple for use by You in connection with Your Applications that are associated with Your developer account.

"**HealthKit APIs**" means the Documented APIs that enable reading, writing, queries and/or retrieval of an end-user's health and/or fitness information in Apple's Health application.

"**HomeKit Accessory Protocol**" means the proprietary protocol licensed by Apple under Apple's MFi/Works with Apple Program that enables home accessories designed to work with the HomeKit APIs (e.g., lights, locks) to communicate with compatible iOS Products, Apple Watch and other supported Apple-branded products.

"**HomeKit APIs**" means the Documented APIs that enable reading, writing, queries and/or retrieval of an end-user's home configuration or home automation information from that end-user's designated area of Apple's HomeKit Database.

"**HomeKit Database**" means Apple's repository for storing and managing information about an end-user's Licensed HomeKit Accessories and associated information.

"**iCloud**" or "**iCloud service**" means the iCloud online service provided by Apple that includes remote online storage.

"**iCloud Storage APIs**" means the Documented APIs that allow storage and/or retrieval of user-generated documents and other files, and allow storage and/or retrieval of key value data (e.g., a list of stocks in a finance App, settings for an App) for Applications and Web Software through the use of iCloud.

"**In-App Purchase API**" means the Documented API that enables additional content, functionality or services to be delivered or made available for use within an Application with or without an additional fee.

"**Intermediary Party**" means a party that passes an Apple Pay end-user's Apple Pay Payload to a Merchant for processing such end-user's payment transaction outside of an Application.

"**iOS**" means the iOS operating system software provided by Apple for use by You only in connection with Your Application development and testing, including any successor versions thereof.

"**iOS Product**" means an Apple-branded product that runs iOS or iPadOS.

"**iPadOS**" means the iPadOS operating system software provided by Apple for use by You only in connection with Your Application development and testing, including any successor versions thereof.

"**iPod Accessory Protocol**" or "**iAP**" means Apple's proprietary protocol for communicating with supported Apple-branded products and which is licensed under the MFi/Works with Apple Program.

"**Library**" means a code module that cannot be installed or executed separately from an Application and that is developed by You in compliance with the Documentation and Program Requirements only for use with iOS Products, Apple Watch, or Apple TV.

"**Licensed Application**" means an Application that (a) meets and complies with all of the Documentation and Program Requirements, and (b) has been selected and digitally signed by Apple for distribution, and includes any additional permitted functionality, content or services provided by You from within an Application using the In-App Purchase API.

"**Licensed Application Information**" means screen shots, images, artwork, previews, icons and/or any other text, descriptions, representations or information relating to a Licensed

Application that You provide to Apple for use in accordance with Schedule 1, or, if applicable, Schedule 2 or Schedule 3.

"**Licensed HomeKit Accessories**" means hardware accessories licensed under the MFi/Works with Apple Program that support the HomeKit Accessory Protocol.

"**Local Notification**" means a message, including any content or data therein, that Your Application delivers to end-users at a pre-determined time or when Your Application is running in the background and another application is running in the foreground.

"**macOS**" means the macOS operating system software provided by Apple for use by You, including any successor versions thereof.

"**MFi Licensee**" means a party who has been granted a license by Apple under the MFi/Works with Apple Program.

"**MFi/Works with Apple Accessory**" or "**MFi Accessory**" means a non-Apple branded hardware device that interfaces, communicates, or otherwise interoperates with or controls an Apple-branded product using technology licensed under the MFi/Works with Apple Program (e.g., the ability to control a supported Apple-branded product through the iPod Accessory Protocol).

"**MFi/Works with Apple Program**" means a separate Apple program that offers developers, among other things, a license to incorporate or use certain Apple technology in or with hardware accessories or devices for purposes of interfacing, communicating or otherwise interoperating with or controlling select Apple-branded products.

"**Map Data**" means any content, data or information provided through the Apple Maps Service including, but not limited to, imagery, terrain data, latitude and longitude coordinates, transit data, points of interest and traffic data.

"**MapKit API**" means the Documented API that enables You to add mapping features or functionality to Applications.

"**MapKit JS**" means the JavaScript library that enables You to add mapping features or functionality to Your Applications, websites, or web applications.

"**Merchant**" means a party who processes Apple Pay payment transactions under their own name, trademark, or brand (e.g., their name shows up on the end-user's credit card statement).

"**Motion & Fitness APIs**" means the Documented APIs that are controlled by the Motion & Fitness privacy setting in a compatible Apple-branded product and that enable access to motion and fitness sensor data (e.g., body motion, step count, stairs climbed), unless the end-user has disabled access to such data.

"**Multitasking**" means the ability of Applications to run in the background while other Applications are also running.

"**MusicKit APIs**" means the set of APIs that enable Apple Music users to access their subscription through Your Application or as otherwise permitted by Apple in the Documentation.

"**MusicKit Content**" means music, video, and/or graphical content rendered through the MusicKit APIs.

"**MusicKit JS**" means the JavaScript library that enables Apple Music users to access their subscription through Your Applications, websites, or web applications.

"**Network Extension Framework**" means the Documented APIs that provide Applications with the ability to customize certain networking features of compatible Apple-branded products (e.g., customizing the authentication process for WiFi Hotspots, VPN features, and content filtering mechanisms).

"**Pass(es)**" means one or more digital passes (e.g., movie tickets, coupons, loyalty reward vouchers, boarding passes, membership cards, etc.) developed by You under this Agreement, under Your own trademark or brand, and which are signed with Your Pass Type ID.

"**Pass Information**" means the text, descriptions, representations or information relating to a Pass that You provide to or receive from Your end-users on or in connection with a Pass.

"**Pass Type ID**" means the combination of an Apple Certificate and Push Application ID that is used by You to sign Your Passes and/or communicate with the APN.

"**Program**" means the overall Apple development, testing, digital signing, and distribution program contemplated in this Agreement.

"**Program Requirements**" mean the technical, human interface, design, product category, security, performance, and other criteria and requirements specified by Apple, including but not limited to the current set of requirements set forth in **Section 3.3**, as they may be modified from time to time by Apple in accordance with this Agreement.

"**Provisioning Profiles**" means the files (including applicable entitlements or other identifiers) that are provided by Apple for use by You in connection with Your Application development and testing, and limited distribution of Your Applications for use on Registered Devices and/or on Authorized Test Units.

"**Push Application ID**" means the unique identification number or other identifier that Apple assigns to an Application, Pass or Site in order to permit it to access and use the APN.

"**Push Notification**" or "**Safari Push Notification**" means a notification, including any content or data therein, that You transmit to end-users for delivery in Your Application, Your Pass, and/or in the case of macOS, to the macOS desktop of users of Your Site who have opted in to receive such messages through Safari on macOS.

"**Registered Devices**" means Apple-branded hardware units owned or controlled by You, or owned by individuals who are affiliated with You, where such Products have been specifically registered with Apple under this Program.

"**Safari Extensions**" means one or more software extensions developed by You under this Agreement only for use with Safari in compliance with this Agreement.

"**Security Solution**" means the proprietary Apple content protection system marketed as Fairplay, to be applied to Licensed Applications distributed on the App Store to administer Apple's standard usage rules for Licensed Applications, as such system and rules may be modified by Apple from time to time.

"**Sign In with Apple**" means the Documented APIs and JavaScript libraries that allow You to log users into Your Application (and Corresponding Products) with their Apple ID or anonymized credentials.

"**SiriKit**" means the set of APIs that allow Your Application to access or provide SiriKit domains, intents, shortcuts, donations, and other related functionality, as set forth in the Documentation.

"**Site**" means a website provided by You under Your own name, trademark or brand.

"**Single Sign-on Specification**" means the Documentation provided by Apple hereunder for the Single Sign-On API, as updated from time to time.

"**Term**" means the period described in **Section 11**.

"**TestFlight**" means Apple's beta testing service for pre-release Applications made available through Apple's TestFlight Application.

"**TestFlight Application**" means Apple's application that enables the distribution of pre-release versions of Your Applications to a limited number of Your Authorized Developers and to a limited number of Beta Testers (as specified in App Store Connect) through TestFlight.

"**TV App API**" means the API documented in the TV App Specification that enables You to provide Apple with TV App Data.

"**TV App Data**" means the data described in the TV App Specification to be provided to Apple through the TV App API.

"**TV App Features**" means functionality accessible via the TV App and/or tvOS, iOS, iPadOS, and/or macOS devices, which functionality provides the user the ability to view customized information and recommendations regarding content and to access such content through the user's apps, and/or provides the user the ability to continue play of previously viewed content.

"**TV App Specification**" means the Documentation provided by Apple hereunder for the TV App API, as updated from time to time.

"**tvOS**" means the tvOS operating system software, including any successor versions thereof.

"**Updates**" means bug fixes, updates, upgrades, modifications, enhancements, supplements, and new releases or versions of the Apple Software or Services, or to any part of the Apple Software or Services.

"**Wallet**" means Apple's application that has the ability to store and display Passes for use on iOS Products, Apple Watch, or Safari on macOS.

"**WatchKit Extension**" means an extension bundled as part of Your Application that accesses the WatchKit framework on iOS to run and display a WatchKit app on the watchOS.

"**watchOS**" means the watchOS operating system software, including any successor versions thereof.

"**Web Software**" means web-based versions of Your software applications that have the same title and substantially equivalent features and functionality as Your Licensed Application (e.g., feature parity).

"**Website Push ID**" means the combination of an Apple Certificate and Push Application ID that is used by You to sign Your Site's registration bundle and/or communicate with the APN.

"**You**" and "**Your**" means and refers to the person(s) or legal entity (whether the company, organization, educational institution, or governmental agency, instrumentality, or department) that has accepted this Agreement under its own developer account and that is using the Apple Software or otherwise exercising rights under this Agreement.

Note: For the sake of clarity, You may authorize contractors to develop Applications on Your behalf, but any such Applications must be owned by You, submitted under Your own developer

account, and distributed as Applications only as expressly permitted herein. You are responsible to Apple for Your contractors' activities under Your account (e.g., adding them to Your team to perform development work for You) and their compliance with this Agreement. Any actions undertaken by Your contractors arising out of this Agreement shall be deemed to have been taken by You, and You (in addition to Your contractors) shall be responsible to Apple for all such actions.

2. Internal Use License and Restrictions

2.1 Permitted Uses and Restrictions; Program services

Subject to the terms and conditions of this Agreement, Apple hereby grants You during the Term, a limited, non-exclusive, personal, revocable, non-sublicensable and non-transferable license to:

(a) Install a reasonable number of copies of the Apple Software provided to You under the Program on Apple-branded products owned or controlled by You, to be used internally by You or Your Authorized Developers for the sole purpose of developing or testing Covered Products designed to operate on the applicable Apple-branded products, except as otherwise expressly permitted in this Agreement;
(b) Make and distribute a reasonable number of copies of the Documentation to Authorized Developers for their internal use only and for the sole purpose of developing or testing Covered Products, except as otherwise expressly permitted in this Agreement;
(c) Install a Provisioning Profile on each of Your Authorized Test Units, up to the number of Authorized Test Units that You have registered and acquired licenses for, to be used internally by You or Your Authorized Developers for the sole purpose of developing and testing Your Applications, except as otherwise expressly permitted in this Agreement;
(d) Install a Provisioning Profile on each of Your Registered Devices, up to the limited number of Registered Devices that You have registered and acquired licenses for, for the sole purpose of enabling the distribution and use of Your Applications on such Registered Devices; and
(e) Incorporate the Apple Certificates issued to You pursuant to this Agreement for purposes of digitally signing Your Applications, Passes, Safari Extensions, Safari Push Notifications, and as otherwise expressly permitted by this Agreement.

Apple reserves the right to set the limited number of Apple-branded products that each Licensee may register with Apple and obtain licenses for under this Program (a "**Block of Registered Device Licenses**"). For the purposes of limited distribution on Registered Devices under **Section 7.3 (Ad Hoc distribution)**, each company, organization, educational institution or affiliated group may only acquire one (1) Block of Registered Device Licenses per company, organization, educational institution or group, unless otherwise agreed in writing by Apple. You agree not to knowingly acquire, or to cause others to acquire, more than one Block of Registered Device Licenses for the same company, organization, educational institution or group.

Apple may provide access to services by or through the Program for You to use with Your developer account (e.g., device or app provisioning, managing teams or other account resources). You agree to access such services only through the Program web portal (which is accessed through Apple's developer website) or through Apple-branded products that are designed to work in conjunction with the Program (e.g., Xcode, App Store Connect) and only as authorized by Apple. If You (or Your Authorized Developers) access Your developer account through these other Apple-branded products, You acknowledge and agree that this Agreement shall continue to apply to any use of Your developer account and to any features or functionality of the Program that are made available to You (or Your Authorized Developers) in this manner (e.g., Apple Certificates and Provisioning Profiles can be used only in the limited manner permitted herein, etc.). You agree not to create or attempt to create a substitute or similar service through use of or access to the services provided by or through the Program. If Apple provides power and performance metrics for Your Application, You agree that such metrics may be used solely for Your own internal use and may not be provided to any third party (except as set forth in **Section 2.9**). Further, You may only access such services using the Apple ID associated with

Your developer account or authentication credentials (e.g., keys, tokens, password) associated with Your developer account, and You are fully responsible for safeguarding Your Apple ID and authentication credentials from compromise and for using them only as authorized by Apple and in accordance with the terms of this Agreement, including but not limited to **Section 2.8** and **5**. Except as otherwise expressly permitted herein, You agree not to share, sell, resell, rent, lease, lend, or otherwise provide access to Your developer account or any services provided therewith, in whole or in part, to anyone who is not an Authorized Developer on Your team, and You agree not to solicit or request Apple Developer Program members to provide You with their Apple IDs, authentication credentials, and/or related account information and materials (e.g., Apple Certificates used for distribution or submission to the App Store or TestFlight). You understand that each team member must have their own Apple ID or authentication credentials to access Your account, and You shall be fully responsible for all activity performed through or in connection with Your account. To the extent that You own or control an Apple-branded computer running Apple's macOS Server or Xcode Server ("**Server**") and would like to use it for Your own development purposes in connection with the Program, You agree to use Your own Apple ID or other authentication credentials for such Server, and You shall be responsible for all actions performed by such Server.

2.2 Authorized Test Units and Pre-Release Apple Software

As long as an Authorized Test Unit contains any pre-release versions of the Apple Software or uses pre-release versions of Services, You agree to restrict access to such Authorized Test Unit to Your Authorized Developers and to not disclose, show, rent, lease, lend, sell or otherwise transfer such Authorized Test Unit to any third party. You further agree to take reasonable precautions to safeguard, and to instruct Your Authorized Developers to safeguard, all Authorized Test Units from loss or theft. Further, subject to the terms of this Agreement, You may deploy Your Applications to Your Authorized Developers for use on a limited number of Authorized Test Units for Your own internal testing and development purposes.

You acknowledge that by installing any pre-release Apple Software or using any pre-release Services on Your Authorized Test Units, these Units may be "locked" into testing mode and may not be capable of being restored to their original condition. Any use of any pre-release Apple Software or pre-release Services are for evaluation and development purposes only, and You should not use any pre-release Apple Software or pre-release Services in a commercial operating environment or with important data. You should back up any data prior to using the pre-release Apple Software or pre-release Services. Apple shall not be responsible for any costs, expenses or other liabilities You may incur as a result of provisioning Your Authorized Test Units and Registered Devices, Your Covered Product development or the installation or use of this Apple Software or any pre-release Apple Services, including but not limited to any damage to any equipment, or any damage, loss, or corruption of any software, information or data.

2.3 Confidential Nature of Pre-Release Apple Software and Services

From time to time during the Term, Apple may provide You with pre-release versions of the Apple Software or Services that constitute Apple Confidential Information and are subject to the confidentiality obligations of this Agreement, except as otherwise set forth herein. Such pre-release Apple Software and Services should not be relied upon to perform in the same manner as a final-release, commercial-grade product, nor used with data that is not sufficiently and regularly backed up, and may include features, functionality or APIs for software or services that are not yet available. You acknowledge that Apple may not have publicly announced the availability of such pre-release Apple Software or Services, that Apple has not promised or guaranteed to You that such pre-release software or services will be announced or made available to anyone in the future, and that Apple has no express or implied obligation to You to announce or commercially introduce such software or services or any similar or compatible technology. You expressly acknowledge and agree that any research or development that You perform with respect to pre-release versions of the Apple Software or Services is done entirely at Your own risk.

2.4 Copies
You agree to retain and reproduce in full the Apple copyright, disclaimers and other proprietary notices (as they appear in the Apple Software and Documentation provided) in all copies of the Apple Software and Documentation that You are permitted to make under this Agreement.

2.5 Ownership
Apple retains all rights, title, and interest in and to the Apple Software, Services, and any Updates it may make available to You under this Agreement. You agree to cooperate with Apple to maintain Apple's ownership of the Apple Software and Services, and, to the extent that You become aware of any claims relating to the Apple Software or Services, You agree to use reasonable efforts to promptly provide notice of any such claims to Apple. The parties acknowledge that this Agreement does not give Apple any ownership interest in Your Covered Products.

2.6 No Other Permitted Uses
Except as otherwise set forth in this Agreement, You agree not to rent, lease, lend, upload to or host on any website or server, sell, redistribute, or sublicense the Apple Software, Apple Certificates, or any Services, in whole or in part, or to enable others to do so. You may not use the Apple Software, Apple Certificates, or any Services provided hereunder for any purpose not expressly permitted by this Agreement, including any applicable Attachments and Schedules. You agree not to install, use or run the Apple SDKs on any non-Apple-branded computer, and not to install, use or run iOS, watchOS, tvOS, iPadOS, macOS and Provisioning Profiles on or in connection with devices other than Apple-branded products, or to enable others to do so. You may not and You agree not to, or to enable others to, copy (except as expressly permitted under this Agreement), decompile, reverse engineer, disassemble, attempt to derive the source code of, modify, decrypt, or create derivative works of the Apple Software, Apple Certificates or any Services provided by the Apple Software or otherwise provided hereunder, or any part thereof (except as and only to the extent any foregoing restriction is prohibited by applicable law or to the extent as may be permitted by licensing terms governing use of open-sourced components or sample code included with the Apple Software). You agree not to exploit any Apple Software, Apple Certificates, or Services provided hereunder in any unauthorized way whatsoever, including but not limited to, by trespass or burdening network capacity, or by harvesting or misusing data provided by such Apple Software, Apple Certificates, or Services. Any attempt to do so is a violation of the rights of Apple and its licensors of the Apple Software or Services. If You breach any of the foregoing restrictions, You may be subject to prosecution and damages. All licenses not expressly granted in this Agreement are reserved and no other licenses, immunity or rights, express or implied are granted by Apple, by implication, estoppel, or otherwise. This Agreement does not grant You any rights to use any trademarks, logos or service marks belonging to Apple, including but not limited to the iPhone or iPod word marks. If You make reference to any Apple products or technology or use Apple's trademarks, You agree to comply with the published guidelines at https://www.apple.com/legal/intellectual-property/guidelinesfor3rdparties.html, as they may be modified by Apple from time to time.

2.7 FPS SDK and FPS Deployment Package
You may use the FPS SDK to develop and test a server-side implementation of FPS, solely for use with video streamed by You (or on Your behalf) through Your Applications, or video downloaded for viewing through Your Applications, on iOS Products and/or Apple TV, through Safari on macOS, or as otherwise approved by Apple in writing (collectively, "**Authorized FPS Applications**"). You understand that You will need to request the FPS Deployment Package on the Program web portal prior to any production or commercial use of FPS. As part of such request, You will need to submit information about Your requested use of FPS. Apple will review Your request and reserves the right to not provide You with the FPS Deployment Package at its sole discretion, in which case You will not be able to deploy FPS. Any development and testing You perform with the FPS SDK is at Your own risk and expense, and Apple will not be liable to You for such use or for declining Your request to use FPS in a production or commercial environment.

If Apple provides You with the FPS Deployment Package, You agree to use it solely as approved by Apple and only in connection with video content streamed by You (or on Your behalf) to Authorized FPS Applications or downloaded for viewing through Your Authorized FPS Applications. Except as permitted in **Section 2.9 (Third-Party Service Providers)**, You will not provide the FPS Deployment Package to any third party or sublicense, sell, resell, lease, disclose, or re-distribute the FPS Deployment Package or FPS SDK to any third party (or any implementation thereof) without Apple's prior written consent.

You acknowledge and agree that the FPS Deployment Package (including the set of FPS production keys) is Apple Confidential Information as set forth in **Section 9 (Confidentiality)**. Further, such FPS keys are unique to Your company or organization, and You are solely responsible for storing and protecting them. You may use such FPS keys solely for the purpose of delivering and protecting Your content key that is used to decrypt video content streamed by You to Authorized FPS Applications or downloaded for viewing through Your Authorized FPS Applications. Apple will have no liability or responsibility for unauthorized access to or use of any FPS key or any content streamed or otherwise delivered under this Agreement in connection with FPS. In the event that Your FPS key is disclosed, discovered, misappropriated or lost, You may request that Apple revoke it by emailing product-security@apple.com, and You understand that Apple will have no obligation to provide a replacement key. Apple reserves the right to revoke Your FPS key at any time if requested by You, in the event of a breach of this Agreement by You, if otherwise deemed prudent or reasonable by Apple, or upon expiration or termination of this Agreement for any reason.

You acknowledge and agree that Apple reserves the right to revoke or otherwise remove Your access to and use of FPS (or any part thereof) at any time in its sole discretion. Further, Apple will have no obligation to provide any modified, updated or successor version of the FPS Deployment Package or the FPS SDK to You and will have no obligation to maintain compatibility with any prior version. If Apple makes new versions of the FPS Deployment Package or FPS SDK available to You, then You agree to update to them within a reasonable time period if requested to do so by Apple.

2.8 Use of Apple Services

Apple may provide access to Apple Services that Your Covered Products may call through APIs in the Apple Software and/or that Apple makes available to You through other mechanisms, e.g., through the use of keys that Apple may make accessible to You under the Program. You agree to access such Apple Services only through the mechanisms provided by Apple for such access and only for use on Apple-branded products. Except as permitted in **Section 2.9 (Third-Party Service Providers)** or as otherwise set forth herein, You agree not to share access to mechanisms provided to You by Apple for the use of the Services with any third party. Further, You agree not to create or attempt to create a substitute or similar service through use of or access to the Apple Services.

You agree to access and use such Services only as necessary for providing services and functionality for Your Covered Products that are eligible to use such Services and only as permitted by Apple in writing, including in the Documentation. You may not use the Apple Services in any manner that is inconsistent with the terms of this Agreement or that infringes any intellectual property rights of a third party or Apple, or that violates any applicable laws or regulations. You agree that the Apple Services contain proprietary content, information and material owned by Apple and its licensors, and protected by applicable intellectual property and other laws. You may not use such proprietary content, information or materials in any way whatsoever, except for the permitted uses of the Apple Services under this Agreement, or as otherwise agreed by Apple in writing.

You understand there may be storage capacity, transmission, and/or transactional limits for the Apple Services both for You as a developer and for Your end-users. If You reach or Your end-

user reaches such limits, then You or Your end-user may be unable to use the Apple Services or may be unable to access or retrieve data from such Services through Your Covered Products or through the applicable end-user accounts. You agree not to charge any fees to end-users solely for access to or use of the Apple Services through Your Covered Products or for any content, data or information provided therein, and You agree not to sell access to the Apple Services in any way. You agree not to fraudulently create any end-user accounts or induce any end-user to violate the terms of their applicable end-user terms or service agreement with Apple or to violate any Apple usage policies for such end-user services. Except as expressly set forth herein, You agree not to interfere with an end-user's ability to access or use any such services.

Apple reserves the right to change, suspend, deprecate, deny, limit, or disable access to the Apple Services, or any part thereof, at any time without notice (including but not limited to revoking entitlements or changing any APIs in the Apple Software that enable access to the Services or not providing You with an entitlement). In no event will Apple be liable for the removal of or disabling of access to any of the foregoing. Apple may also impose limits and restrictions on the use of or access to the Apple Services, may remove the Apple Services for indefinite time periods, may revoke Your access to the Apple Services, or may cancel the Apple Services (or any part thereof) at any time without notice or liability to You and in its sole discretion.

Apple does not guarantee the availability, accuracy, completeness, reliability, or timeliness of any data or information displayed by any Apple Services. To the extent You choose to use the Apple Services with Your Covered Products, You are responsible for Your reliance on any such data or information. You are responsible for Your use of the Apple Software and Apple Services, and if You use such Services, then it is Your responsibility to maintain appropriate alternate backup of all Your content, information and data, including but not limited to any content that You may provide to Apple for hosting as part of Your use of the Services. You understand and agree that You may not be able to access certain Apple Services upon expiration or termination of this Agreement and that Apple reserves the right to suspend access to or delete content, data or information that You or Your Covered Product have stored through Your use of such Services provided hereunder. You should review the Documentation and policy notices posted by Apple prior to using any Apple Services.

Apple Services may not be available in all languages or in all countries, and Apple makes no representation that any such Services would be appropriate, accurate or available for use in any particular location or product. To the extent You choose to use the Apple Services with Your Applications, You do so at Your own initiative and are responsible for compliance with any applicable laws. Apple reserves the right to charge fees for Your use of the Apple Services. Apple will inform You of any Apple Service fees or fee changes by email and information about such fees will be posted in the Program web portal, App Store Connect, or the CloudKit dashboard. Apple Service availability and pricing are subject to change. Further, Apple Services may not be made available for all Covered Products and may not be made available to all developers. Apple reserves the right to not provide (or to cease providing) the Apple Services to any or all developers at any time in its sole discretion.

2.9 Third-Party Service Providers

Unless otherwise prohibited by Apple in the Documentation or this Agreement, You are permitted to employ or retain a third party ("**Service Provider**") to assist You in using the Apple Software and Services provided pursuant to this Agreement, including, but not limited to, engaging any such Service Provider to maintain and administer Your Applications' servers on Your behalf, provided that any such Service Provider's use of the Apple Software and Services or any materials associated therewith is done solely on Your behalf and only in accordance with these terms. Notwithstanding the foregoing, You may not use a Service Provider to submit an Application to the App Store or use TestFlight on Your behalf. You agree to have a binding written agreement with Your Service Provider with terms at least as restrictive and protective of Apple as those set forth herein. Any actions undertaken by any such Service Provider in relation

to Your Applications or use of the Apple Software or Apple Services and/or arising out of this Agreement shall be deemed to have been taken by You, and You (in addition to the Service Provider) shall be responsible to Apple for all such actions (or any inactions). In the event of any actions or inactions by the Service Provider that would constitute a violation of this Agreement or otherwise cause any harm, Apple reserves the right to require You to cease using such Service Provider.

2.10 Updates; No Support or Maintenance

Apple may extend, enhance, or otherwise modify the Apple Software or Services (or any part thereof) provided hereunder at any time without notice, but Apple shall not be obligated to provide You with any Updates to the Apple Software or Services. If Updates are made available by Apple, the terms of this Agreement will govern such Updates, unless the Update is accompanied by a separate license in which case the terms of that license will govern. You understand that such modifications may require You to change or update Your Covered Products. Further, You acknowledge and agree that such modifications may affect Your ability to use, access, or interact with the Apple Software and Services. Apple is not obligated to provide any maintenance, technical or other support for the Apple Software or Services. You acknowledge that Apple has no express or implied obligation to announce or make available any Updates to the Apple Software or to any Services to anyone in the future. Should an Update be made available, it may have APIs, features, services or functionality that are different from those found in the Apple Software licensed hereunder or the Services provided hereunder.

3. Your Obligations

3.1 General

You certify to Apple and agree that:

(a) You are of the legal age of majority in the jurisdiction in which You reside (at least 18 years of age in many countries) and have the right and authority to enter into this Agreement on Your own behalf, or if You are entering into this Agreement on behalf of Your company, organization, educational institution, or agency, instrumentality, or department of the federal government, that You have the right and authority to legally bind such entity or organization to the terms and obligations of this Agreement;

(b) All information provided by You to Apple or Your end-users in connection with this Agreement or Your Covered Products, including without limitation Licensed Application Information or Pass Information, will be current, true, accurate, supportable and complete and, with regard to information You provide to Apple, You will promptly notify Apple of any changes to such information. Further, You agree that Apple may share such information (including email address and mailing address) with third parties who have a need to know for purposes related thereto (e.g., intellectual property questions, customer service inquiries, etc.);

(c) You will comply with the terms of and fulfill Your obligations under this Agreement, including obtaining any required consents for Your Authorized Developers' use of the Apple Software and Services, and You agree to monitor and be fully responsible for all such use by Your Authorized Developers and their compliance with the terms of this Agreement;

(d) You will be solely responsible for all costs, expenses, losses and liabilities incurred, and activities undertaken by You and Your Authorized Developers in connection with the Apple Software and Apple Services, the Authorized Test Units, Registered Devices, Your Covered Products and Your related development and distribution efforts, including, but not limited to, any related development efforts, network and server equipment, Internet service(s), or any other hardware, software or services used by You in connection with Your use of any services;

(e) For the purposes of Schedule 1 (if applicable), You represent and warrant that You own or control the necessary rights in order to appoint Apple and Apple Subsidiaries as Your worldwide agent for the delivery of Your Licensed Applications, and that the fulfillment of such appointment by Apple and Apple Subsidiaries shall not violate or infringe the rights of any third party; and

(f) You will not act in any manner which conflicts or interferes with any existing commitment or obligation You may have and no agreement previously entered into by You will interfere with Your performance of Your obligations under this Agreement.

3.2 Use of the Apple Software and Apple Services

As a condition to using the Apple Software and any Apple Services, You agree that:

(a) You will use the Apple Software and any services only for the purposes and in the manner expressly permitted by this Agreement and in accordance with all applicable laws and regulations;

(b) You will not use the Apple Software or any Apple Services for any unlawful or illegal activity, nor to develop any Covered Product, which would commit or facilitate the commission of a crime, or other tortious, unlawful or illegal act;

(c) Your Application, Library and/or Pass will be developed in compliance with the Documentation and the Program Requirements, the current set of which is set forth in **Section 3.3** below;

(d) To the best of Your knowledge and belief, Your Covered Products, Licensed Application Information, and Pass Information do not and will not violate, misappropriate, or infringe any Apple or third party copyrights, trademarks, rights of privacy and publicity, trade secrets, patents, or other proprietary or legal rights (e.g., musical composition or performance rights, video rights, photography or image rights, logo rights, third party data rights, etc. for content and materials that may be included in Your Application);

(e) You will not, through use of the Apple Software, Apple Certificates, Apple Services or otherwise, create any Covered Product or other code or program that would disable, hack or otherwise interfere with the Security Solution, or any security, digital signing, digital rights management, verification or authentication mechanisms implemented in or by iOS, watchOS, iPadOS, tvOS, the Apple Software, or any Services, or other Apple software or technology, or enable others to do so (except to the extent expressly permitted by Apple in writing);

(f) You will not, directly or indirectly, commit any act intended to interfere with the Apple Software or Services, the intent of this Agreement, or Apple's business practices including, but not limited to, taking actions that may hinder the performance or intended use of the App Store, Custom App Distribution, or the Program (e.g., submitting fraudulent reviews of Your own Application or any third party application, choosing a name for Your Application that is substantially similar to the name of a third party application in order to create consumer confusion, or squatting on application names to prevent legitimate third party use). Further, You will not engage, or encourage others to engage, in any unlawful, unfair, misleading, fraudulent, improper, or dishonest acts or business practices relating to Your Covered Products (e.g., engaging in bait-and-switch pricing, consumer misrepresentation, deceptive business practices, or unfair competition against other developers); and

(g) Applications for iOS Products, Apple Watch, or Apple TV developed using the Apple Software may be distributed only if selected by Apple (in its sole discretion) for distribution via the App Store, Custom App Distribution, for beta distribution through TestFlight, or through Ad Hoc distribution as contemplated in this Agreement. Passes developed using the Apple Software may be distributed to Your end-users via email, a website or an Application in accordance with the terms of this Agreement, including Attachment 5. Safari Extensions signed with an Apple Certificate may be distributed to Your end-users in accordance with the terms of this Agreement, including Attachment 7. Applications for macOS may be distributed outside of the App Store using Apple Certificates and/or tickets as set forth in **Section 5.3** and **5.4**.

3.3 Program Requirements

Any Application that will be submitted to the App Store, Custom App Distribution, or TestFlight, or that will be distributed through Ad Hoc distribution, must be developed in compliance with the Documentation and the Program Requirements, the current set of which is set forth below in this **Section 3.3**. Libraries and Passes are subject to the same criteria:

APIs and Functionality:

3.3.1 Applications may only use Documented APIs in the manner prescribed by Apple and must not use or call any private APIs. Further, macOS Applications submitted to Apple for distribution on the App Store may use only Documented APIs included in the default installation of macOS or as bundled with Xcode and the Mac SDK; deprecated technologies (such as Java)

may not be used.

3.3.2 Except as set forth in the next paragraph, an Application may not download or install executable code. Interpreted code may be downloaded to an Application but only so long as such code: (a) does not change the primary purpose of the Application by providing features or functionality that are inconsistent with the intended and advertised purpose of the Application as submitted to the App Store, (b) does not create a store or storefront for other code or applications, and (c) does not bypass signing, sandbox, or other security features of the OS.

An Application that is a programming environment intended for use in learning how to program may download and run executable code so long as the following requirements are met: (i) no more than 80 percent of the Application's viewing area or screen may be taken over with executable code, except as otherwise permitted in the Documentation, (ii) the Application must present a reasonably conspicuous indicator to the user within the Application to indicate that the user is in a programming environment, (iii) the Application must not create a store or storefront for other code or applications, and (iv) the source code provided by the Application must be completely viewable and editable by the user (e.g., no pre-compiled libraries or frameworks may be included with the code downloaded).

3.3.3 Without Apple's prior written approval or as permitted under **Section 3.3.25** (**In-App Purchase API**), an Application may not provide, unlock or enable additional features or functionality through distribution mechanisms other than the App Store, Custom App Distribution or TestFlight.

3.3.4 An Application for iOS, watchOS, iPadOS, or tvOS may only read data from or write data to an Application's designated container area on the device, except as otherwise specified by Apple. For macOS Applications submitted to Apple for distribution on the App Store: (a) all files necessary for the Application to execute on macOS must be in the Application bundle submitted to Apple and must be installed by the App Store; (b) all localizations must be in the same Application bundle and may not include a suite or collection of independent applications within a single Application bundle; (c) native user interface elements or behaviors of macOS (e.g., the system menu, window sizes, colors, etc.) may not be altered, modified or otherwise changed; (d) You may not use any digital rights management or other copy or access control mechanisms in such Applications without Apple's written permission or as specified in the Documentation; and (e) except as otherwise permitted by **Section 3.3.25** (**In-App Purchase API**), such Applications may not function as a distribution mechanism for software and may not include features or functionality that create or enable a software store, distribution channel or other mechanism for software delivery within such Applications (e.g., an audio application may not include an audio filter plug-in store within the Application).

3.3.5 An Application for an iOS Product must have at least the same features and functionality when run by a user in compatibility mode on an iPad (e.g., an iPhone app running in an equivalent iPhone-size window on an iPad must perform in substantially the same manner as when run on the iPhone; provided that this obligation will not apply to any feature or functionality that is not supported by a particular hardware device, such as a video recording feature on a device that does not have a camera). Further, You agree not to interfere or attempt to interfere with the operation of Your Application in compatibility mode.

3.3.6 You may use the Multitasking services only for their intended purposes as described in the Documentation.

User Interface, Data Collection, Local Laws and Privacy:

3.3.7 Applications must comply with the Human Interface Guidelines (HIG) and other Documentation provided by Apple. You agree to follow the HIG to develop an appropriate user interface and functionality for Your Application that is compatible with the design of Apple-

branded products (e.g., a watch App should have a user interface designed for quick interactions in accordance with the HIG's watchOS design themes).

3.3.8 If Your Application captures or makes any video, microphone, screen recordings, or camera recordings, whether saved on the device or sent to a server (e.g., an image, photo, voice or speech capture, or other recording) (collectively "**Recordings**"), a reasonably conspicuous audio, visual or other indicator must be displayed to the user as part of the Application to indicate that a Recording is taking place.

- In addition, any form of data, content or information collection, processing, maintenance, uploading, syncing, storage, transmission, sharing, disclosure or use performed by, through or in connection with Your Application must comply with all applicable privacy laws and regulations as well as any related Program Requirements, including but not limited to any notice or consent requirements.

3.3.9 You and Your Applications (and any third party with whom You have contracted to serve advertising) may not collect user or device data without prior user consent, whether such data is obtained directly from the user or through the use of the Apple Software, Apple Services, or Apple SDKs, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising in accordance with **Sections 3.3.12**. You may not broaden or otherwise change the scope of usage for previously collected user or device data without obtaining prior user consent for such expanded or otherwise changed data collection. You may not use analytics software in Your Application to collect and send device data to a third party. Further, neither You nor Your Application will use any permanent, device-based identifier, or any data derived therefrom, for purposes of uniquely identifying a device.

3.3.10 You must provide clear and complete information to users regarding Your collection, use and disclosure of user or device data, e.g., a description of Your use of user and device data in the App Description on the App Store. Furthermore, You must take appropriate steps to protect such data from unauthorized use, disclosure or access by third parties. If a user ceases to consent or affirmatively revokes consent for Your collection, use or disclosure of his or her user or device data, You (and any third party with whom You have contracted to serve advertising) must promptly cease all such use. You must provide a privacy policy in Your Application, on the App Store, and/or on Your website explaining Your collection, use, disclosure, sharing, retention, and deletion of user or device data. You agree to notify Your users, in accordance with applicable law, in the event of a data breach in which user data collected from Your Application is compromised (e.g., You will send an email notifying Your users if there has been an unintentional disclosure or misuse of their user data).

3.3.11 Applications must comply with all applicable criminal, civil and statutory laws and regulations, including those in any jurisdictions in which Your Applications may be offered or made available. In addition:

- You and the Application must comply with all applicable privacy and data collection laws and regulations with respect to any collection, use or disclosure of user or device data (e.g., a user's IP address, the name of the user's device, and any installed apps associated with a user);

- Applications may not be designed or marketed for the purpose of harassing, abusing, spamming, stalking, threatening or otherwise violating the legal rights (such as the rights of privacy and publicity) of others;

- Neither You nor Your Application may perform any functions or link to any content, services, information or data or use any robot, spider, site search or other retrieval application or device to scrape, mine, retrieve, cache, analyze or index software, data or services provided by Apple or its licensors, or obtain (or try to obtain) any such data, except the data that Apple expressly provides

or makes available to You in connection with such services. You agree that You will not collect, disseminate or use any such data for any unauthorized purpose; and

- If Your Application is intended for human subject research or uses the HealthKit APIs for clinical health-related uses which may involve personal data (e.g., storage of health records), then You agree to inform participants of the intended uses and disclosures of their personally identifiable data as part of such research or clinical health uses and to obtain consent from such participants (or their guardians) who will be using Your Application for such research or clinical health purposes. Further, You shall prohibit third parties to whom You provide any de-identified or coded data from re-identifying (or attempting to re-identify) any participants using such data without participant consent, and You agree to require that such third parties pass the foregoing restriction on to any other parties who receive such de-identified or coded data.

Advertising Identifier and Preference; Ad Network APIs:

3.3.12 You and Your Applications (and any third party with whom You have contracted to serve advertising) may use the Advertising Identifier, and any information obtained through the use of the Advertising Identifier, only for the purpose of serving advertising. If a user resets the Advertising Identifier, then You agree not to combine, correlate, link or otherwise associate, either directly or indirectly, the prior Advertising Identifier and any derived information with the reset Advertising Identifier. For Applications compiled for any Apple-branded product providing access to the Ad Support APIs, You agree to check a user's Advertising Preference prior to serving any advertising using the Advertising Identifier, and You agree to abide by a user's setting in the Advertising Preference in Your use of the Advertising Identifier. In addition, You may request to use the Ad Network APIs to track application advertising conversion events. If You are granted permission to use the Ad Network APIs, You agree not to use such APIs, or any information obtained through the use of the Ad Network APIs, for any purpose other than verifying ad validation information as part of an advertising conversion event. You agree not to combine, correlate, link, or otherwise associate, either directly or indirectly, information that is provided as part of the ad validation through the use of the Ad Network APIs with other information You may have about a user. Apple reserves the right to reject any requests to use the Ad Network APIs, in its sole discretion.

Location and Maps; User Consents:

3.3.13 Applications that use location-based APIs (e.g., Core Location, MapKit API) or otherwise provide location-based services may not be designed or marketed for automatic or autonomous control of vehicle behavior, or for emergency or life-saving purposes.

3.3.14 Applications that offer location-based services or functionality, or that otherwise obtain a user's location through the use of the Apple Software or Apple Services, must notify and obtain consent from an individual before his or her location data is collected, transmitted or otherwise used by the Application and then such data must be used only as consented to by the user and as permitted herein. For example, if You use the "Always" location option in Your Application for the purpose of continuous collection and use of a user's location data, You should provide a clearly defined justification and user benefit that is presented to the user at the time of the permission.

3.3.15 If You choose to provide Your own location-based service, data and/or information in conjunction with the Apple maps provided through the Apple Maps Service (e.g., overlaying a map or route You have created on top of an Apple map), You are solely responsible for ensuring that Your service, data and/or information correctly aligns with any Apple maps used. For Applications that use location-based APIs for real-time navigation (including, but not limited to, turn-by-turn route guidance and other routing that is enabled through the use of a sensor), You must have an end-user license agreement that includes the following notice: YOUR USE OF

THIS REAL TIME ROUTE GUIDANCE APPLICATION IS AT YOUR SOLE RISK. LOCATION DATA MAY NOT BE ACCURATE.

3.3.16 Applications must not disable, override or otherwise interfere with any Apple-implemented system alerts, warnings, display panels, consent panels and the like, including, but not limited to, those that are intended to notify the user that the user's location data, address book data, calendar, photos, audio data, and/or reminders are being collected, transmitted, maintained, processed or used, or intended to obtain consent for such use. Further, if You have the ability to add a description in such alerts, warnings, and display panels (e.g., information in the purpose strings for the Camera APIs), any such description must be accurate and not misrepresent the scope of use. If consent is denied or withdrawn, Applications may not collect, transmit, maintain, process or utilize such data or perform any other actions for which the user's consent has been denied or withdrawn.

3.3.17 If Your Application (or Your website or web application, as applicable) uses or accesses the MapKit API or MapKit JS from a device running iOS version 6 or later, Your Application (or Your website or web application, as applicable) will access and use the Apple Maps Service. All use of the MapKit API, MapKit JS, and Apple Maps Service must be in accordance with the terms of this Agreement (including the Program Requirements) and Attachment 6 (Additional Terms for the use of the Apple Maps Service).

Content and Materials:

3.3.18 Any master recordings and musical compositions embodied in Your Application must be wholly-owned by You or licensed to You on a fully paid-up basis and in a manner that will not require the payment of any fees, royalties and/or sums by Apple to You or any third party. In addition, if Your Application will be distributed outside of the United States, any master recordings and musical compositions embodied in Your Application (a) must not fall within the repertoire of any mechanical or performing/communication rights collecting or licensing organization now or in the future and (b) if licensed, must be exclusively licensed to You for Your Application by each applicable copyright owner.

3.3.19 If Your Application includes or will include any other content, You must either own all such content or have permission from the content owner to use it in Your Application.

3.3.20 Applications may be rejected if they contain content or materials of any kind (text, graphics, images, photographs, sounds, etc.) that in Apple's reasonable judgment may be found objectionable or inappropriate, for example, materials that may be considered obscene, pornographic, or defamatory.

3.3.21 Applications must not contain any malware, malicious or harmful code, program, or other internal component (e.g., computer viruses, trojan horses, "backdoors") which could damage, destroy, or adversely affect the Apple Software, services, Apple-branded products, or other software, firmware, hardware, data, systems, services, or networks.

3.3.22 If Your Application includes any FOSS, You agree to comply with all applicable FOSS licensing terms. You also agree not to use any FOSS in the development of Your Application in such a way that would cause the non-FOSS portions of the Apple Software to be subject to any FOSS licensing terms or obligations.

3.3.23 Your Application may include promotional sweepstake or contest functionality provided that You are the sole sponsor of the promotion and that You and Your Application comply with any applicable laws and fulfill any applicable registration requirements in the country or territory where You make Your Application available and the promotion is open. You agree that You are solely responsible for any promotion and any prize, and also agree to clearly state in binding

official rules for each promotion that Apple is not a sponsor of, or responsible for conducting, the promotion.

3.3.24 Your Application may include a direct link to a page on Your web site where You include the ability for an end-user to make a charitable contribution, provided that You comply with any applicable laws (which may include providing a receipt), and fulfill any applicable regulation or registration requirements, in the country or territory where You enable the charitable contribution to be made. You also agree to clearly state that Apple is not the fundraiser.

In-App Purchase API:

3.3.25 All use of the In-App Purchase API and related services must be in accordance with the terms of this Agreement (including the Program Requirements) and Attachment 2 (Additional Terms for Use of the In-App Purchase API).

Network Extension Framework:

3.3.26 Your Application must not access the Network Extension Framework unless Your Application is primarily designed for providing networking capabilities, and You have received an entitlement from Apple for such access. You agree to the following if You receive such entitlement:

- You agree to clearly disclose to end-users how You and Your Application will be using their network information and, if applicable, filtering their network data, and You agree to use such data and information only as expressly consented to by the end-user and as expressly permitted herein;

- You agree to store and transmit network information or data from an end-user in a secure and appropriate manner;

- You agree not to divert an end-user's network data or information through any undisclosed, improper, or misleading processes, e.g., to filter it through a website to obtain advertising revenue or spoof a website;

- You agree not to use any network data or information from end-users to bypass or override any end-user settings, e.g., You may not track an end-user's WiFi network usage to determine their location if they have disabled location services for Your Application; and

- Notwithstanding anything to the contrary in **Section 3.3.9**, You and Your Application may not use the Network Extension Framework, or any data or information obtained through the Network Extension Framework, for any purpose other than providing networking capabilities in connection with Your Application (e.g., not for using an end-user's Internet traffic to serve advertising or to otherwise build user profiles for advertising).

Apple reserves the right to not provide You with an entitlement to use the Network Extension Framework in its sole discretion and to revoke such entitlement at any time. In addition, if You would like to use the Access WiFi Information APIs (which provide the WiFi network to which a device is connected), then You must request an entitlement from Apple for such use, and, notwithstanding anything to the contrary in **Section 3.3.9**, You may use such APIs only for providing a service or function that is directly relevant to the Application (e.g., not for serving advertising).

MFi Accessories:

3.3.27 Your Application may interface, communicate, or otherwise interoperate with or control an MFi Accessory (as defined above) through wireless transports or through Apple's lightning or 30-

pin connectors only if (i) such MFi Accessory is licensed under Apple's MFi/Works with Apple Program at the time that You initially submit Your Application, (ii) the MFi Licensee has added Your Application to a list of those approved for interoperability with their MFi Accessory, and (iii) the MFi Licensee has received approval from the Apple MFi/Works with Apple Program for such addition.

Regulatory Compliance:

3.3.28 You will fulfill any applicable regulatory requirements, including full compliance with all applicable laws, regulations, and policies related to the manufacturing, marketing, sale and distribution of Your Application in the United States, and in particular the requirements of the U.S. Food and Drug Administration (FDA) as well as other U.S. regulatory bodies such as the FAA, HHS, FTC, and FCC, and the laws, regulations and policies of any other applicable regulatory bodies in any countries or territories where You use or make Your Application available, e.g., MHRA, CFDA. However, You agree that You will not seek any regulatory marketing permissions or make any determinations that may result in any Apple products being deemed regulated or that may impose any obligations or limitations on Apple. By submitting Your Application to Apple for selection for distribution, You represent and warrant that You are in full compliance with any applicable laws, regulations, and policies, including but not limited to all FDA laws, regulations and policies, related to the manufacturing, marketing, sale and distribution of Your Application in the United States, as well as in other countries or territories where You plan to make Your Application available. You also represent and warrant that You will market Your Application only for its cleared or approved intended use/indication for use, and only in strict compliance with applicable regulatory requirements. Upon Apple's request, You agree to promptly provide any such clearance documentation to support the marketing of Your Application. If requested by the FDA or by another government body that has a need to review or test Your Application as part of its regulatory review process, You may provide Your Application to such entity for review purposes. You agree to promptly notify Apple in accordance with the procedures set forth in **Section 14.5** of any complaints or threats of complaints regarding Your Application in relation to any such regulatory requirements, in which case Apple may remove Your Application from distribution.

Cellular Network:

3.3.29 If an Application requires or will have access to the cellular network, then additionally such Application:

- Must comply with Apple's best practices and other guidelines on how Applications should access and use the cellular network; and

- Must not in Apple's reasonable judgment excessively use or unduly burden network capacity or bandwidth.

3.3.30 Because some mobile network operators may prohibit or restrict the use of Voice over Internet Protocol (VoIP) functionality over their network, such as the use of VoIP telephony over a cellular network, and may also impose additional fees, or other charges in connection with VoIP. You agree to inform end-users, prior to purchase, to check the terms of agreement with their operator, for example, by providing such notice in the marketing text that You provide accompanying Your Application on the App Store. In addition, if Your Application allows end-users to send SMS messages or make cellular voice calls, then You must inform the end-user, prior to use of such functionality, that standard text messaging rates or other carrier charges may apply to such use.

Apple Push Notification Service and Local Notifications:

3.3.31 All use of Push Notifications via the Apple Push Notification Service or Local Notifications must be in accordance with the terms of this Agreement (including the Program Requirements) and Attachment 1 (Additional Terms for Apple Push Notification Service and Local Notifications).

Game Center:

3.3.32 All use of the Game Center must be in accordance with the terms of this Agreement (including the Program Requirements) and Attachment 3 (Additional Terms for the Game Center).

iCloud:

3.3.33 All use of the iCloud Storage APIs and CloudKit APIs, as well as Your use of the iCloud service under this Agreement, must be in accordance with the terms of this Agreement (including the Program Requirements) and Attachment 4 (Additional Terms for the use of iCloud).

Wallet:

3.3.34 Your development of Passes, and use of the Pass Type ID and Wallet under this Agreement, must be in accordance with the terms of this Agreement (including the Program Requirements) and Attachment 5 (Additional Terms for Passes).

Additional Services or End-User Pre-Release Software:

3.3.35 From time to time, Apple may provide access to additional Services or pre-release Apple Software for You to use in connection with Your Applications, or as an end-user for evaluation purposes. Some of these may be subject to separate terms and conditions in addition to this Agreement, in which case Your usage will also be subject to those terms and conditions. Such services or software may not be available in all languages or in all countries, and Apple makes no representation that they will be appropriate or available for use in any particular location. To the extent You choose to access such services or software, You do so at Your own initiative and are responsible for compliance with any applicable laws, including but not limited to applicable local laws. To the extent any such software includes Apple's FaceTime or Messages feature, You acknowledge and agree that when You use such features, the telephone numbers and device identifiers associated with Your Authorized Test Units, as well as email addresses and/or Apple ID information You provide, may be used and maintained by Apple to provide and improve such software and features. Certain services made accessible to You through the Apple Software may be provided by third parties. You acknowledge that Apple will not have any liability or responsibility to You or any other person (including to any end-user) for any third-party services or for any Apple services. Apple and its licensors reserve the right to change, suspend, remove, or disable access to any services at any time. In no event will Apple be liable for the removal or disabling of access to any such services. Further, upon any commercial release of such software or services, or earlier if requested by Apple, You agree to cease all use of the pre-release Apple Software or Services provided to You as an end-user for evaluation purposes under this Agreement.

3.3.36 If Your Application accesses the Google Safe Browsing service through the Apple Software such access is subject to Google's terms of service set forth at: https://developers.google.com/safe-browsing/terms. If You do not accept such terms of service, then You may not use the Google Safe Browsing Service in Your Application, and You acknowledge and agree that such use will constitute Your acceptance of such terms of service.

3.3.37 If Your Application accesses data from an end-user's Address Book through the Address Book API, You must notify and obtain consent from the user before his or her Address Book data is accessed or used by Your Application. Further, Your Application may not provide an automated mechanism that transfers only the Facebook Data portions of the end-user's Address Book altogether to a location off of the end-user's device. For the sake of clarity, this does not

prohibit an automated transfer of the user's entire Address Book as a whole, so long as user notification and consent requirements have been fulfilled; and does not prohibit enabling users to transfer any portion of their Address Book data manually (e.g., by cutting and pasting) or enabling them to individually select particular data items to be transferred.

Extensions:

3.3.38 Applications that include extensions in the Application bundle must provide some functionality beyond just the extensions (e.g., help screens, additional settings), unless an Application includes a WatchKit Extension. In addition:

- Extensions (excluding WatchKit Extensions) may not include advertising, product promotion, direct marketing, or In-App Purchase offers in their extension view;

- Extensions may not block the full screen of an iOS Product or Apple TV, or redirect, obstruct or interfere in an undisclosed or unexpected way with a user's use of another developer's application or any Apple-provided functionality or service;

- Extensions may operate only in Apple-designated areas of iOS, watchOS, iPadOS, or tvOS as set forth in the Documentation;

- Extensions that provide keyboard functionality must be capable of operating independent of any network access and must include Unicode characters (vs. pictorial images only);

- Any keystroke logging done by any such extension must be clearly disclosed to the end-user prior to any such data being sent from an iOS Product, and notwithstanding anything else in **Section 3.3.9**, such data may be used only for purposes of providing or improving the keyboard functionality of Your Application (e.g., not for serving advertising);

- Any message filtering done by an extension must be clearly disclosed to the end-user, and notwithstanding anything else in **Section 3.3.9**, any SMS or MMS data (whether accessed through a message filtering extension or sent by iOS to a messaging extension's corresponding server) may be used only for purposes of providing or improving the message experience of the user by reducing spam or messages from unknown sources, and must not be used for serving advertising or for any other purpose. Further, SMS or MMS data from a user that is accessed within the extension may not be exported from the extension's designated container area in any way; and

- Your Application must not automate installation of extensions or otherwise cause extensions to be installed without the user's knowledge, and You must accurately specify to the user the purpose and functionality of the extension.

HealthKit APIs and Motion & Fitness APIs:

3.3.39 Your Application must not access the HealthKit APIs or Motion & Fitness APIs unless it is primarily designed to provide health, motion, and/or fitness services, and this usage is clearly evident in Your marketing text and user interface. In addition:

- Notwithstanding anything to the contrary in **Section 3.3.9**, You and Your Application may not use the HealthKit APIs or the Motion & Fitness APIs, or any information obtained through the HealthKit APIs or the Motion & Fitness APIs, for any purpose other than providing health, motion, and/or fitness services in connection with Your Application (e.g., not for serving advertising);

- You must not use the HealthKit APIs or the Motion & Fitness APIs, or any information obtained through the HealthKit APIs or the Motion & Fitness APIs, to disclose or provide an end-user's health, motion, and/or fitness information to a third party without prior express end-user consent,

and then only for purposes of enabling the third party to provide health, motion, and/or fitness services as permitted herein. For example, You must not share or sell an end-user's health information collected through the HealthKit APIs or Motion & Fitness APIs to advertising platforms, data brokers, or information resellers. For clarity, You may allow end-users to consent to share their data with third parties for medical research purposes; and

- You agree to clearly disclose to end-users how You and Your Application will be using their health, motion, and/or fitness information and to use it only as expressly consented to by the end-user and as expressly permitted herein.

Configuration Profiles:

3.3.40 Configuration Profiles cannot be delivered to consumers other than for the purposes of configuration of WiFi, APN, or VPN settings, or as otherwise expressly permitted by Apple in the then-current Configuration Profile Reference Documentation. You must make a clear declaration of what user data will be collected and how it will be used on an app screen or other notification mechanism prior to any user action to use a Configuration Profile. You may not share or sell user data obtained through a Configuration Profile to advertising platforms, data brokers, or information resellers. In addition, You may not override the consent panel for a Configuration Profile or any other mechanisms of a Configuration Profile.

HomeKit APIs:

3.3.41 Your Application must not access the HomeKit APIs unless it is primarily designed to provide home configuration or home automation services (e.g., turning on a light, lifting a garage door) for Licensed HomeKit Accessories and this usage is clearly evident in Your marketing text and user interface. You agree not to use the HomeKit APIs for any purpose other than interfacing, communicating, interoperating with or otherwise controlling a Licensed HomeKit Accessory or for using the HomeKit Database, and then only for home configuration or home automation purposes in connection with Your Application. In addition:

- Your Application may use information obtained from the HomeKit APIs and/or the HomeKit Database only on a compatible Apple-branded product and may not export, remotely access or transfer such information off of the applicable product (e.g., a lock password cannot be sent off an end-user's device to be stored in an external non-Apple database), unless otherwise expressly permitted by Apple in the Documentation; and

- Notwithstanding anything to the contrary in **Section 3.3.9**, You and Your Application may not use the HomeKit APIs, or any information obtained through the HomeKit APIs or through the HomeKit Database, for any purpose other than providing or improving home configuration or home automation services in connection with Your Application (e.g., not for serving advertising).

Apple Pay APIs:

3.3.42 Your Application may use the Apple Pay APIs solely for the purpose of facilitating payment transactions that are made by or through Your Application, and only for the purchase of goods and services that are to be used outside of any iOS Product or Apple Watch, unless otherwise permitted by Apple in writing. For clarity, nothing in this **Section 3.3.42** supplants any of the rules or requirements for the use of the In-App Purchase API, including but not limited to **Section 3.3.3** and the guidelines. In addition:

- You acknowledge and agree that Apple is not a party to any payment transactions facilitated through the use of the Apple Pay APIs and is not responsible for any such transactions, including but not limited to the unavailability of any end-user payment cards or payment fraud. Such payment transactions are between You and Your bank, acquirer, card networks, or other parties You utilize for transaction processing, and You are responsible for complying with any

agreements You have with such third parties. In some cases, such agreements may contain terms specifying specific rights, obligations or limitations that You accept and assume in connection with Your decision to utilize the functionality of the Apple Pay APIs;

- You agree to store any private keys provided to You as part of Your use of the Apple Pay APIs in a secure manner (e.g., encrypted on a server) and in accordance with the Documentation. You agree not to store any end-user payment information in an unencrypted manner on an iOS Product. For clarity, You may not decrypt any such end-user payment information on an iOS Product;

- You agree not to call the Apple Pay APIs or otherwise attempt to gain information through the Apple Pay APIs for purposes unrelated to facilitating end-user payment transactions; and

- If You use Apple Pay APIs in Your Application, then You agree to use commercially reasonable efforts to include Apple Pay Cash as a payment option with Your use of the Apple Pay APIs in accordance with the Documentation and provided that Apple Pay Cash is available in the jurisdiction in which the Application is distributed.

3.3.43 As part of facilitating an end-user payment transaction through the Apple Pay APIs, Apple may provide You (whether You are acting as the Merchant or as an Intermediary Party) with an Apple Pay Payload. If You receive an Apple Pay Payload, then You agree to the following:

- If You are acting as the Merchant, then You may use the Apple Pay Payload to process the end-user payment transaction and for other uses that You disclose to the end-user, and only in accordance with applicable law; and

- If You are acting as an Intermediary Party, then:

(a) You may use the Apple Pay Payload only for purposes of facilitating the payment transaction between the Merchant and the end-user and for Your own order management purposes (e.g., customer service) as part of such transaction;
(b) You agree that You will not hold the Apple Pay Payload data for any longer than necessary to fulfill the payment transaction and order management purposes for which it was collected;
(c) You agree not to combine data obtained through the Apple Pay APIs, including but not limited to, the Apple Pay Payload with any other data that You may have about such end-user (except to the limited extent necessary for order management purposes). For clarity, an Intermediary Party may not use data obtained through the Apple Pay APIs for advertising or marketing purposes, for developing or enhancing a user profile, or to otherwise target end-users;
(d) You agree to disclose to end-users that You are an Intermediary Party to the transaction and to provide the identity of the Merchant for a particular transaction on the Apple Pay Payment Sheet (in addition to including Your name as an Intermediary Party); and
(e) If You use a Merchant, then You will be responsible for ensuring that the Merchant You select uses the Apple Pay Payload provided by You only for purposes of processing the end-user payment transaction and for other uses they have disclosed to the end-user, and only in accordance with applicable law. You agree to have a binding written agreement with such Merchant with terms at least as restrictive and protective of Apple as those set forth herein. Any actions undertaken by any such Merchant in relation to such Apple Pay Payload or the payment transaction shall be deemed to have been taken by You, and You (in addition to such Merchant) shall be responsible to Apple for all such actions (or any inactions). In the event of any actions or inactions by such Merchant that would constitute a violation of this Agreement or otherwise cause any harm, Apple reserves the right to require You to cease using such Merchant.

SiriKit:

3.3.44 Your Application may register as a destination to use the Apple-defined SiriKit domains, but only if Your Application is designed to provide relevant responses to a user, or otherwise

carry out the user's request or intent, in connection with the applicable SiriKit domain (e.g., ride sharing) that is supported by Your Application and this usage is clearly evident in Your marketing text and user interface. In addition, Your Application may contribute actions to SiriKit, but only if such actions are tied to user behavior or activity within Your Application and for which You can provide a relevant response to the user. You agree not to submit false information through SiriKit about any such user activity or behavior or otherwise interfere with the predictions provided by SiriKit (e.g., SiriKit donations should be based on actual user behavior).

3.3.45 Your Application may use information obtained through SiriKit only on supported Apple products and may not export, remotely access or transfer such information off a device except to the extent necessary to provide or improve relevant responses to a user or carry out a user's request or in connection with Your Application. Notwithstanding anything to the contrary in **Section 3.3.9**, You and Your Application may not use SiriKit, or any information obtained through SiriKit, for any purpose other than providing relevant responses to a user or otherwise carrying out a user's request or intent in connection with an SiriKit domain, intent, or action supported by Your Application and/or for improving Your Application's responsiveness to user requests (e.g., not for serving advertising).

3.3.46 If Your Application uses SiriKit to enable audio data to be processed by Apple, You agree to clearly disclose to end-users that You and Your Application will be sending their recorded audio data to Apple for speech recognition, processing and/or transcription purposes, and that such audio data may be used to improve and provide Apple products and services. You further agree to use such audio data, and recognized text that may be returned from SiriKit, only as expressly consented to by the end-user and as expressly permitted herein.

Single Sign-On API:

3.3.47 You must not access or use the Single Sign-On API unless You are a Multi-channel Video Programming Distributor (MVPD) or unless Your Application is primarily designed to provide authenticated video programming via a subscription-based MVPD service, and You have received an entitlement from Apple to use the Single Sign-On API. If You have received such an entitlement, You are permitted to use the Single Sign-On API solely for the purpose of authenticating a user's entitlement to access Your MVPD content for viewing on an Apple Product, in accordance with the Single Sign-on Specification. Any such use must be in compliance with the Documentation for the Single Sign-On Specification. You acknowledge that Apple reserves the right to not provide You such an entitlement, and to revoke such entitlement, at any time, in its sole discretion.

If You use the Single Sign-On API, You will be responsible for providing the sign-in page accessed by users via the Single Sign-On API where users sign in to authenticate their right to access Your MVPD content. You agree that such sign-in page will not display advertising, and that the content and appearance of such page will be subject to Apple's prior review and approval. If You use the Single Sign-On API and Apple provides an updated version of such API and/or the Single Sign-on Specification, You agree to update Your implementation to conform with the newer version and specification within 3 months after receiving the update from Apple.

You authorize Apple to use, reproduce, and display the trademarks provided by You for use in connection with the Single-Sign-On feature, including use in the user interface screens in Apple products where the user selects the provider and authenticates through Single Sign-on, and/or to provide the user with a list of apps that are accessible to such user through Single Sign-On. You also grant Apple the right to use screen shots and images of such user interface, including but not limited to use in instructional materials, training materials, marketing materials, and advertising in any medium. Data provided via the Single Sign-On API will be considered Licensed Application Information hereunder, but will be subject to the use limitations set forth in this Section.

You must not collect, store or use data provided via the Single Sign-On API for any purpose other

than to authenticate a user's entitlement to access Your MVPD content on an Apple product, to provide the user access to Your MVPD content, and/or to address performance and technical problems with Your MVPD service. You will not provide or disclose data, content or information obtained from use of the Single Sign-On API to any other party except for authentication information provided to a video programming provider whose programming is offered as part of an MVPD subscription offered by You, and solely for the purpose of authenticating the user's entitlement to access such video programming on an Apple product under the user's MVPD subscription.

TV App API:

3.3.48 You may not use the TV App API unless (a) Your Application is primarily designed to provide video programming, (b) You have received an entitlement from Apple, and (c) Your use is in accordance with the TV App Specification. To the extent that You provide TV App Data to Apple, Apple may store, use, reproduce and display such data solely for the purposes of: (a) providing information and recommendations to users of TV App Features, (b) enabling users to link from such recommendations and/or information to content for viewing via Your Licensed Application, and/or (c) servicing, maintenance, and optimization of TV App Features. With respect to any TV App Data that has been submitted by You prior to termination of this Agreement, Apple may continue to use such data in accordance with this **Section 3.3.48** after termination of this Agreement. TV App Data will be considered Licensed Application Information under this Agreement, but will be subject to the use limitations set forth in this Section. You acknowledge that Apple reserves the right to not include Your Licensed Application in the TV App Features, in its sole discretion.

Apple will obtain user consent based on the user's Apple ID before including Your Licensed Application in the TV App Features displayed under that Apple ID. Apple will also provide users with the ability to withdraw such consent at any time thereafter and to delete their TV App Data from Apple's systems. In addition, You may solicit user consent based upon Your own subscriber ID system. You are responsible for Your compliance with all applicable laws, including any applicable local laws for obtaining user consent with respect to Your provision of TV App Data to Apple.

Spotlight-Image-Search Service:

3.3.49 To the extent that You provide Apple's spotlight-image-search service with access to any of Your domains that are associated with Your Licensed Applications (the "Associated Domain(s)"), You hereby grant Apple permission to crawl, scrape, copy, transmit and/or cache the content found in the Associated Domain(s) (the "Licensed Content") for the purposes set forth in this section. The Licensed Content shall be considered Licensed Application Information under this Agreement. You hereby further grant Apple a license to use, make, have made, reproduce, crop and/or modify the file format, resolution and appearance of the Licensed Content (for the purposes of reducing file size, converting to a supported file type and/or displaying thumbnails), and to publicly display, publicly perform, integrate, incorporate and distribute the Licensed Content to enhance search, discovery, and end-user distribution of the Licensed Content in Apple's Messages feature. Upon the termination of this Agreement for any reason, end users of Apple-branded products will be permitted to continue using and distributing all Licensed Content that they obtained through the use of Apple-branded products prior to such termination.

MusicKit:

3.3.50 You agree not to call the MusicKit APIs or use MusicKit JS (or otherwise attempt to gain information through the MusicKit APIs or MusicKit JS) for purposes unrelated to facilitating access to Your end users' Apple Music subscriptions. If You access the MusicKit APIs or MusicKit JS, then You must follow the Apple Music Identity Guidelines. You agree not to require payment for or indirectly monetize access to the Apple Music service (e.g. in-app purchase,

advertising, requesting user info) through Your use of the MusicKit APIs, MusicKit JS, or otherwise in any way. In addition:

- If You choose to offer music playback through the MusicKit APIs or MusicKit JS, full songs must be enabled for playback, and users must initiate playback and be able to navigate playback using standard media controls such as “play,” “pause,” and “skip”, and You agree to not misrepresent the functionality of these controls;

- You may not, and You may not permit Your end users to, download, upload, or modify any MusicKit Content and MusicKit Content cannot be synchronized with any other content, unless otherwise permitted by Apple in the Documentation;

- You may play MusicKit Content only as rendered by the MusicKit APIs or MusicKit JS and only as permitted in the Documentation (e.g., album art and music-related text from the MusicKit API may not be used separately from music playback or managing playlists);

- Metadata from users (such as playlists and favorites) may be used only to provide a service or function that is clearly disclosed to end users and that is directly relevant to the use of Your Application, website, or web application, as determined in Apple’s sole discretion; and

- You may use MusicKit JS only as a stand-alone library in Your Application, website, or web application and only as permitted in the Documentation (e.g., You agree not to recombine MusicKit JS with any other JavaScript code or separately download and re-host it).

DeviceCheck APIs:

3.3.51 If You use DeviceCheck APIs to store DeviceCheck Data, then You must provide a mechanism for customers to contact You to reset those values, if applicable (e.g. resetting a trial subscription or re-authorizing certain usage when a new user acquires the device). You may not rely on the DeviceCheck Data as a single identifier of fraudulent conduct and must use the DeviceCheck Data only in connection with other data or information, e.g., the DeviceCheck Data cannot be the sole data point since a device may have been transferred or resold. Apple reserves the right to delete any DeviceCheck Data at any time in its sole discretion, and You agree not to rely on any such Data. Further, You agree not to share the DeviceCheck tokens You receive from Apple with any third party, except a Service Provider acting on Your behalf.

Face Data:

3.3.52 If Your Application accesses Face Data, then You must do so only to provide a service or function that is directly relevant to the use of the Application, and You agree to inform users of Your intended uses and disclosures of Face Data by Your Application and to obtain clear and conspicuous consent from such users before any collection or use of Face Data. Notwithstanding anything to the contrary in **Section 3.3.9**, neither You nor Your Application (nor any third party with whom You have contracted to serve advertising) may use Face Data for serving advertising or for any other unrelated purposes. In addition:

- You may not use Face Data in a manner that will violate the legal rights of Your users (or any third parties) or to provide an unlawful, unfair, misleading, fraudulent, improper, exploitative, or objectionable user experience and then only in accordance with the Documentation;

- You may not use Face Data for authentication, advertising, or marketing purposes, or to otherwise target an end-user in a similar manner;

- You may not use Face Data to build a user profile, or otherwise attempt, facilitate, or encourage third parties to identify anonymous users or reconstruct user profiles based on Face Data;

- You agree not to transfer, share, sell, or otherwise provide Face Data to advertising platforms, analytics providers, data brokers, information resellers or other such parties; and

- Face Data may not be shared or transferred off the user's device unless You have obtained clear and conspicuous consent for the transfer and the Face Data is used only in fulfilling a specific service or function for Your Application (e.g., a face mesh is used to display an image of the user within the Application) and only in accordance with these terms and the Documentation. You agree to require that Your service providers use Face Data only to the limited extent consented to by the user and only in accordance with these terms.

ClassKit APIs:

3.3.53 Your Application must not include the ClassKit APIs unless it is primarily designed to provide educational services, and this usage is clearly evident in Your marketing text and user interface. You agree not to submit false or inaccurate data through the ClassKit APIs or to attempt to redefine the assigned data categories for data submitted through the ClassKit APIs (e.g., student location data is not a supported data type and should not be submitted).

Sign In with Apple:

3.3.54 You may use Sign In with Apple in Your Corresponding Products only so long as Your use is comparable to including Sign In with Apple in Your Application. You may not share or sell user data obtained through Sign In with Apple to advertising platforms, data brokers, or information resellers. If a user has chosen to anonymize their user data as part of Sign In with Apple, You agree not to attempt to link such anonymized data with information that directly identifies the individual and that is obtained outside of Sign In with Apple without first obtaining user consent.

4. Changes to Program Requirements or Terms

Apple may change the Program Requirements or the terms of this Agreement at any time. New or modified Program Requirements will not retroactively apply to Applications already in distribution via the App Store or Custom App Distribution; provided however that You agree that Apple reserves the right to remove Applications from the App Store or Custom App Distribution that are not in compliance with the new or modified Program Requirements at any time. In order to continue using the Apple Software, Apple Certificates or any Services, You must accept and agree to the new Program Requirements and/or new terms of this Agreement. If You do not agree to new Program Requirements or new terms, Your use of the Apple Software, Apple Certificates and any Services will be suspended or terminated by Apple. You agree that Your acceptance of such new Agreement terms or Program Requirements may be signified electronically, including without limitation, by Your checking a box or clicking on an "agree" or similar button. Nothing in this Section shall affect Apple's rights under **Section 5 (Apple Certificates; Revocation)**.

5. Apple Certificates; Revocation

5.1 Certificate Requirements

All Applications must be signed with an Apple Certificate in order to be installed on Authorized Test Units, Registered Devices, or submitted to Apple for distribution via the App Store, Custom App Distribution, or TestFlight. Similarly, all Passes must be signed with an Apple Certificate to be recognized and accepted by Wallet. Safari Extensions must be signed with an Apple Certificate to run in Safari on macOS. You must use a Website ID to send Safari Push Notifications to the macOS desktop of users who have opted in to receive such Notifications for Your Site through Safari on macOS. You may also obtain other Apple Certificates and keys for other purposes as set forth herein and in the Documentation.

In relation to this, You represent and warrant to Apple that:

(a) You will not take any action to interfere with the normal operation of any Apple Certificates, keys, or Provisioning Profiles;
(b) You are solely responsible for preventing any unauthorized person or organization from having access to Your Apple Certificates and keys, and You will use Your best efforts to safeguard Your Apple Certificates and keys from compromise (e.g., You will not upload Your Apple Certificate for App Store distribution to a cloud repository for use by a third-party);
(c) You agree to immediately notify Apple in writing if You have any reason to believe there has been a compromise of any of Your Apple Certificates or keys;
(d) You will not provide or transfer Apple Certificates or keys provided under this Program to any third party (except for a Service Provider who is using them on Your behalf in compliance with this Agreement and only to the limited extent expressly permitted by Apple in the Documentation or this Agreement (e.g., You are prohibited from providing or transferring Your Apple Certificates that are used for distribution or submission to the App Store to a Service Provider), and You will not use Your Apple Certificates to sign any third party's application, pass, extension, notification, implementation, or site;
(e) You will use any Apple Certificates or keys provided under this Agreement solely as permitted by Apple and in accordance with the Documentation; and
(f) You will use Apple Certificates provided under this Program exclusively for the purpose of signing Your Passes, signing Your Safari Extensions, signing Your Site's registration bundle, accessing the APN service, and/or signing Your Applications for testing, submission to Apple and/or for limited distribution for use on Registered Devices or Authorized Test Units as contemplated under this Program, or as otherwise permitted by Apple, and only in accordance with this Agreement. As a limited exception to the foregoing, You may provide versions of Your Applications to Your Service Providers to sign with their Apple-issued development certificates, but solely for purposes of having them perform testing on Your behalf of Your Applications on Apple-branded products running iOS, watchOS, iPadOS, and/or tvOS and provided that all such testing is conducted internally by Your Service Providers (e.g., no outside distribution of Your Applications) and that Your Applications are deleted within a reasonable period of time after such testing is performed. Further, You agree that Your Service Provider may use the data obtained from performing such testing services only for purposes of providing You with information about the performance of Your Applications (e.g., Your Service Provider is prohibited from aggregating Your Applications' test results with other developers' test results).

You further represent and warrant to Apple that the licensing terms governing Your Application, Your Safari Extension, Your Site's registration bundle, and/or Your Pass, or governing any third party code or FOSS included in Your Covered Products, will be consistent with and not conflict with the digital signing or content protection aspects of the Program or any of the terms, conditions or requirements of the Program or this Agreement. In particular, such licensing terms will not purport to require Apple (or its agents) to disclose or make available any of the keys, authorization codes, methods, procedures, data or other information related to the Security Solution, digital signing or digital rights management mechanisms or security utilized as part of any Apple software, including the App Store. If You discover any such inconsistency or conflict, You agree to immediately notify Apple of it and will cooperate with Apple to resolve such matter. You acknowledge and agree that Apple may immediately cease distribution of any affected Licensed Applications or Passes, and may refuse to accept any subsequent Application or Pass submissions from You until such matter is resolved to Apple's reasonable satisfaction.

5.2 Relying Party Certificates

The Apple Software and Services may also contain functionality that permits digital certificates, either Apple Certificates or other third-party certificates, to be accepted by the Apple Software or Services (e.g., Apple Pay) and/or to be used to provide information to You (e.g., transaction receipts, App Attest receipts). It is Your responsibility to verify the validity of any certifications or receipts You may receive from Apple prior to relying on them (e.g., You should verify that the receipt came from Apple prior to any delivery of content to an end-user through the use of the In-App Purchase API). You are solely responsible for Your decision to rely on any such certificates and receipts, and Apple will not be liable for Your failure to verify that any such certificates or

receipts came from Apple (or third parties) or for Your reliance on Apple Certificates or other digital certificates.

5.3 Notarized Applications for macOS

To have Your macOS Application notarized, You may request a digital file for authentication of Your Application from Apple's digital notary service (a "**Ticket**"). You can use this Ticket with Your Apple Certificate to receive an improved developer signing and user experience for Your Application on macOS. To request this Ticket from Apple's digital notary service, You must upload Your Application to Apple through Apple's developer tools (or other requested mechanisms) for purposes of continuous security checking. This continuous security checking will involve automated scanning, testing, and analysis of Your Application by Apple for malware or other harmful or suspicious code or components or security flaws, and, in limited cases, a manual, technical investigation of Your Application by Apple for such purposes. By uploading Your Application to Apple for this digital notary service, You agree that Apple may perform such security checks on Your Application for purposes of detecting malware or other harmful or suspicious code or components, and You agree that Apple may retain and use Your Application for subsequent security checks for the same purposes.

If Apple authenticates Your developer signature and Your Application passes the initial security checks, Apple may provide You with a Ticket to use with Your Apple Certificate. Apple reserves the right to issue Tickets in its sole discretion, and Apple may revoke Tickets at any time in its sole discretion in the event that Apple has reason to believe, or has reasonable suspicions, that Your Application contains malware or malicious, suspicious or harmful code or components or that Your developer identity signature has been compromised. You may request that Apple revoke Your Ticket at any time by emailing: product-security@apple.com. If Apple revokes Your Ticket or Your Apple Certificate, then Your Application may no longer run on macOS.

You agree to cooperate with Apple regarding Your Ticket requests and to not hide, attempt to bypass, or misrepresent any part of Your Application from Apple's security checks or otherwise hinder Apple from being able to perform such security checks. You agree not to represent that Apple has performed a security check or malware detection for Your Application or that Apple has reviewed or approved Your Application for purposes of issuing a Ticket to You from Apple's digital notary service. You acknowledge and agree that Apple is performing security checks solely in connection with Apple's digital notary service and that such security checks should not be relied upon for malware detection or security verification of any kind. You are fully responsible for Your own Application and for ensuring that Your Application is safe, secure, and operational for Your end-users (e.g., informing Your end-users that Your Application may cease to run if there is an issue with malware). You agree to comply with export requirements in Your jurisdiction when uploading Your Application to Apple, and You agree not to upload any Application that is: (a) subject to International Traffic in Arms Regulations; or (b) that cannot be exported without prior written government authorization, including, but not limited to, certain types of encryption software and source code, without first obtaining that authorization. Apple will not be liable to You or any third-party for any inability or failure to detect any malware or other suspicious, harmful code or components in Your Application or other security issues, or for any ticket issuance or revocation. Apple shall not be responsible for any costs, expenses, damages, losses or other liabilities You may incur as a result of Your Application development, use of the Apple Software, Apple Services (including this digital notary service), or Apple Certificates, tickets, or participation in the Program, including without limitation the fact that Apple performs security checks on Your Application.

5.4 Certificate Revocation

Except as otherwise set forth herein, You may revoke Apple Certificates issued to You at any time. If You want to revoke the Apple Certificates used to sign Your Passes and/or issued to You for use with Your macOS Applications distributed outside of the App Store, You may request that Apple revoke these Apple Certificates at any time by emailing: product-security@apple.com. Apple also reserves the right to revoke any Apple Certificates at any time, in its sole discretion. By way of example only, Apple may choose to do this if: (a) any of Your Apple Certificates or

corresponding private keys have been compromised or Apple has reason to believe that either have been compromised; (b) Apple has reason to believe or has reasonable suspicions that Your Covered Products contain malware or malicious, suspicious or harmful code or components (e.g., a software virus); (c) Apple has reason to believe that Your Covered Products adversely affect the security of Apple-branded products, or any other software, firmware, hardware, data, systems, or networks accessed or used by such products; (d) Apple's certificate issuance process is compromised or Apple has reason to believe that such process has been compromised; (e) You breach any term or condition of this Agreement; (f) Apple ceases to issue the Apple Certificates for the Covered Product under the Program; (g) Your Covered Product misuses or overburdens any Services provided hereunder; or (h) Apple has reason to believe that such action is prudent or necessary. Further, You understand and agree that Apple may notify end-users of Covered Products that are signed with Apple Certificates when Apple believes such action is necessary to protect the privacy, safety or security of end-users, or is otherwise prudent or necessary as determined in Apple's reasonable judgment. Apple's Certificate Policy and Certificate Practice Statements may be found at: http://www.apple.com/certificateauthority.

6. Application Submission and Selection

6.1 Submission to Apple for App Store or Custom App Distribution

You may submit Your Application for consideration by Apple for distribution via the App Store or Custom App Distribution once You decide that Your Application has been adequately tested and is complete. By submitting Your Application, You represent and warrant that Your Application complies with the Documentation and Program Requirements then in effect as well as with any additional guidelines that Apple may post on the Program web portal or in App Store Connect. You further agree that You will not attempt to hide, misrepresent or obscure any features, content, services or functionality in Your submitted Applications from Apple's review or otherwise hinder Apple from being able to fully review such Applications. In addition, You agree to inform Apple in writing through App Store Connect if Your Application connects to a physical device, including but not limited to an MFi Accessory, and, if so, to disclose the means of such connection (whether iAP, Bluetooth Low Energy (BLE), the headphone jack, or any other communication protocol or standard) and identify at least one physical device with which Your Application is designed to communicate. If requested by Apple, You agree to provide access to or samples of any such devices at Your expense (samples will not be returned). You agree to cooperate with Apple in this submission process and to answer questions and provide information and materials reasonably requested by Apple regarding Your submitted Application, including insurance information You may have relating to Your Application, the operation of Your business, or Your obligations under this Agreement. Apple may require You to carry certain levels of insurance for certain types of Applications and name Apple as an additional insured. If You make any changes to an Application (including to any functionality made available through use of the In-App Purchase API) after submission to Apple, You must resubmit the Application to Apple. Similarly all bug fixes, updates, upgrades, modifications, enhancements, supplements to, revisions, new releases and new versions of Your Application must be submitted to Apple for review in order for them to be considered for distribution via the App Store or Custom App Distribution, except as otherwise permitted by Apple.

6.2 App Thinning and Bundled Resources

As part of Your Application submission to the App Store or Custom App Distribution, Apple may optimize Your Application to target specific devices by repackaging certain functionality and delivered resources (as described in the Documentation) in Your Application so that it will run more efficiently and use less space on target devices ("**App Thinning**"). For example, Apple may deliver only the 32-bit or 64-bit version of Your Application to a target device, and Apple may not deliver icons or launch screens that would not render on the display of a target device. You agree that Apple may use App Thinning to repackage Your Application in order to deliver a more optimized version of Your Application to target devices.

As part of App Thinning, You can also request that Apple deliver specific resources for Your Application (e.g., GPU resources) to target devices by identifying such bundled resources as part of Your code submission ("**Bundled Resources**"). You can define such Bundled Resources to vary the timing or delivery of assets to a target device (e.g., when a user reaches a certain level of a game, then the content is delivered on-demand to the target device). App Thinning and Bundled Resources are not available for all Apple operating systems, and Apple may continue to deliver full Application binaries to some target devices.

6.3 iOS and iPadOS apps on Mac

If You compile Your Application for iOS or iPadOS (collectively "iOS" for purposes of this Section 6.3) and submit such Application for distribution on the App Store, You agree that Apple will make Your Application available on both iOS and macOS via the App Store, unless You choose to opt out of making Your Application available on macOS by following the opt out process in App Store Connect. You agree that the foregoing applies to an Application for iOS submitted by You and currently available on the App Store and to any future Application compiled for iOS and submitted by You to the App Store. Notwithstanding the foregoing, such availability on the App Store will apply only if such Application has been selected by Apple for distribution on the App Store pursuant to Section 7 and only if such Application can function appropriately on, and be compatible with, macOS, as determined in Apple's sole discretion. You are responsible for obtaining and determining if You have appropriate rights for Your Application to operate on macOS. If You do not have such rights, You agree to opt out of making such Application available on macOS. You are responsible for testing such Application on macOS.

6.4 Bitcode Submissions

For Application submissions to the App Store or Custom App Distribution for some Apple operating systems (e.g., for watchOS), Apple may require You to submit an intermediate representation of Your Application in binary file format for the LLVM compiler ("**Bitcode**"). You may also submit Bitcode for other supported Apple operating systems. Such Bitcode submission will allow Apple to compile Your Bitcode to target specific Apple-branded devices and to recompile Your Bitcode for subsequent releases of Your Application for new Apple hardware, software, and/or compiler changes. When submitting Bitcode, You may choose whether or not to include symbols for Your Application in the Bitcode; however, if You do not include symbols, then Apple will not be able to provide You with symbolicated crash logs or other diagnostic information as set forth in **Section 6.6 (Improving Your Application)** below. Further, You may be required to submit a compiled binary of Your Application with Your Bitcode.

By submitting Bitcode to Apple, You authorize Apple to compile Your Bitcode into a resulting binary that will be targeted for specific Apple-branded devices and to recompile Your Bitcode for subsequent rebuilding and recompiling of Your Application for updated hardware, software, and/or compiler changes (e.g., if Apple releases a new device, then Apple may use Your Bitcode to update Your Application without requiring resubmission). You agree that Apple may compile such Bitcode for its own internal use in testing and improving Apple's developer tools, and for purposes of analyzing and improving how applications can be optimized to run on Apple's operating systems (e.g., which frameworks are used most frequently, how a certain framework consumes memory, etc.). You may use Apple's developer tools to view and test how Apple may process Your Bitcode into machine code binary form. Bitcode is not available for all Apple operating systems.

6.5 TestFlight Submission

If You would like to distribute Your Application to Beta Testers outside of Your company or organization through TestFlight, You must first submit Your Application to Apple for review. By submitting such Application, You represent and warrant that Your Application complies with the Documentation and Program Requirements then in effect as well as with any additional guidelines that Apple may post on the Program web portal or in App Store Connect. Thereafter, Apple may permit You to distribute updates to such Application directly to Your Beta Testers without Apple's review, unless such an update includes significant changes, in which case You

agree to inform Apple in App Store Connect and have such Application re-reviewed. Apple reserves the right to require You to cease distribution of Your Application through TestFlight, and/or to any particular Beta Tester, at any time in its sole discretion.

6.6 Improving Your Application
Further, if Your Application is submitted for distribution via the App Store, Custom App Distribution or TestFlight, You agree that Apple may use Your Application for the limited purpose of compatibility testing of Your Application with Apple products and services, for finding and fixing bugs and issues in Apple products and services and/or Your Applications, for internal use in evaluating iOS, watchOS, tvOS, iPadOS, and/or macOS performance issues in or with Your Application, for security testing, and for purposes of providing other information to You (e.g., crash logs). Except as otherwise set forth herein, You may opt in to send app symbol information for Your Application to Apple, and if You do so, then You agree that Apple may use such symbols to symbolicate Your Application for purposes of providing You with symbolicated crash logs and other diagnostic information. In the event that Apple provides You with crash logs or other diagnostic information for Your Application, You agree to use such crash logs and information only for purposes of fixing bugs and improving the performance of Your Application and related products. You may also collect numeric strings and variables from Your Application when it crashes, so long as You collect such information only in an anonymous, non-personal manner and do not recombine, correlate, or use such information to attempt to identify or derive information about any particular end-user or device.

6.7 App Analytics
To the extent that Apple provides an Analytics service through App Store Connect for Applications distributed through the App Store, You agree to use any data provided through such App Analytics service solely for purposes of improving Your Applications and related products. Further, You agree not to provide such information to any third parties, except for a Service Provider who is assisting You in processing and analyzing such data on Your behalf and who is not permitted to use it for any other purpose or disclose it to any other party. For clarity, You must not aggregate (or permit any third-party to aggregate) analytics information provided to You by Apple for Your Applications as part of this App Analytics service with other developers' analytics information, or contribute such information to a repository for cross-developer analytics. You must not use the App Analytics service or any analytics data to attempt to identify or derive information about any particular end-user or device.

6.8 Compatibility Requirement with Current Shipping OS Version
Applications that are selected for distribution via the App Store must be compatible with the currently shipping version of Apple's applicable operating system (OS) software at the time of submission to Apple, and such Applications must stay current and maintain compatibility with each new release of the applicable OS version so long as such Applications are distributed through the App Store. You understand and agree that Apple may remove Applications from the App Store when they are not compatible with the then-current shipping release of the OS at any time in its sole discretion.

6.9 Selection by Apple for Distribution
You understand and agree that if You submit Your Application to Apple for distribution via the App Store, Custom App Distribution, or TestFlight, Apple may, in its sole discretion:

(a) determine that Your Application does not meet all or any part of the Documentation or Program Requirements then in effect;
(b) reject Your Application for distribution for any reason, even if Your Application meets the Documentation and Program Requirements; or
(c) select and digitally sign Your Application for distribution via the App Store, Custom App Distribution, or TestFlight.

Apple shall not be responsible for any costs, expenses, damages, losses (including without limitation lost business opportunities or lost profits) or other liabilities You may incur as a result of Your Application development, use of the Apple Software, Apple Services, or Apple Certificates or participation in the Program, including without limitation the fact that Your Application may not be selected for distribution via the App Store or Custom App Distribution. You will be solely responsible for developing Applications that are safe, free of defects in design and operation, and comply with applicable laws and regulations. You will also be solely responsible for any documentation and end-user customer support and warranty for such Applications. The fact that Apple may have reviewed, tested, approved or selected an Application will not relieve You of any of these responsibilities.

7. Distribution of Applications and Libraries

Applications:

Applications developed under this Agreement for iOS, watchOS, iPadOS, or tvOS may be distributed in four ways: (1) through the App Store, if selected by Apple, (2) through the Custom App Distribution, if selected by Apple, (3) through Ad Hoc distribution in accordance with **Section 7.3**, and (4) for beta testing through TestFlight in accordance with **Section 7.4**. Applications for macOS may be submitted to Apple for selection and distribution on the App Store, or may be separately distributed.

7.1 Delivery of Free Licensed Applications via the App Store or Custom App Distribution

If Your Application qualifies as a Licensed Application, it is eligible for delivery to end-users via the App Store or Custom App Distribution by Apple and/or an Apple Subsidiary. If You would like Apple and/or an Apple Subsidiary to deliver Your Licensed Application or authorize additional content, functionality or services You make available in Your Licensed Application through the use of the In-App Purchase API to end-users for free (no charge) via the App Store or Custom App Distribution, then You appoint Apple and Apple Subsidiaries as Your legal agent and/or commissionaire pursuant to the terms of Schedule 1 for Licensed Applications designated by You as free-of-charge applications.

7.2 Schedule 2 and Schedule 3 for Fee-Based Licensed Applications; Receipts

If Your Application qualifies as a Licensed Application and You intend to charge end-users a fee of any kind for Your Licensed Application or within Your Licensed Application through the use of the In-App Purchase API, You must enter into a separate agreement (Schedule 2) with Apple and/or an Apple Subsidiary before any such commercial distribution of Your Licensed Application may take place via the App Store or before any such commercial delivery of additional content, functionality or services for which You charge end-users a fee may be authorized through the use of the In-App Purchase API in Your Licensed Application. If You would like Apple to sign and distribute Your Application for a fee through Custom App Distribution, then You must enter into a separate agreement (Schedule 3) with Apple and/or an Apple Subsidiary before any such distribution may take place. To the extent that You enter (or have previously entered) into Schedule 2 or Schedule 3 with Apple and/or an Apple Subsidiary, the terms of Schedule 2 or 3 will be deemed incorporated into this Agreement by this reference.

When an end-user installs Your Licensed Application, Apple will provide You with a transaction receipt signed with an Apple Certificate. It is Your responsibility to verify that such certificate and receipt were issued by Apple, as set forth in the Documentation. You are solely responsible for Your decision to rely on any such certificates and receipts. YOUR USE OF OR RELIANCE ON SUCH CERTIFICATES AND RECEIPTS IN CONNECTION WITH A PURCHASE OF A LICENSED APPLICATION IS AT YOUR SOLE RISK. APPLE MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, AS TO MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, ACCURACY, RELIABILITY, SECURITY, OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS WITH RESPECT TO SUCH APPLE

CERTIFICATES AND RECEIPTS. You agree that You will only use such receipts and certificates in accordance with the Documentation, and that You will not interfere or tamper with the normal operation of such digital certificates or receipts, including but not limited to any falsification or other misuse.

7.3 Distribution on Registered Devices (Ad Hoc Distribution)
Subject to the terms and conditions of this Agreement, You may also distribute Your Applications for iOS, watchOS, iPadOS, and tvOS to individuals within Your company, organization, educational institution, group, or who are otherwise affiliated with You for use on a limited number of Registered Devices (as specified on the Program web portal), if Your Application has been digitally signed using Your Apple Certificate as described in this Agreement. By distributing Your Application in this manner on Registered Devices, You represent and warrant to Apple that Your Application complies with the Documentation and Program Requirements then in effect and You agree to cooperate with Apple and to answer questions and provide information about Your Application, as reasonably requested by Apple. You also agree to be solely responsible for determining which individuals within Your company, organization, educational institution or affiliated group should have access to and use of Your Applications and Registered Devices, and for managing such Registered Devices. Apple shall not be responsible for any costs, expenses, damages, losses (including without limitation lost business opportunities or lost profits) or other liabilities You may incur as a result of distributing Your Applications in this manner, or for Your failure to adequately manage, limit or otherwise control the access to and use of Your Applications and Registered Devices. You will be responsible for attaching or otherwise including, at Your discretion, any relevant usage terms with Your Applications. Apple will not be responsible for any violations of Your usage terms. You will be solely responsible for all user assistance, warranty and support of Your Applications.

7.4 TestFlight Distribution
A. Internal Distribution to Authorized Developers and App Store Connect users
You may use TestFlight for internal distribution of pre-release versions of Your Applications to a limited number of Your Authorized Developers or Your App Store Connect users who are members of Your company or organization, but solely for their internal use in testing, evaluating and/or developing Your Applications. Apple reserves the right to require You to cease distribution of such Applications to Your Authorized Developers or Your App Store Connect users through TestFlight, or to any particular Authorized Developer or App Store Connect user, at any time in its sole discretion.

B. External Distribution to Beta Testers
You may also use TestFlight for external distribution of pre-release versions of Your Applications to a limited number of Beta Testers (as specified in App Store Connect), but solely for their testing and evaluation of such pre-release versions of Your Applications and only if Your Application has been approved for such distribution by Apple as set forth in **Section 6.5 (TestFlight Submission)**. You may not charge Your Beta Testers fees of any kind to participate in Apple's TestFlight or for the use of any such pre-release versions. You may not use TestFlight for purposes that are not related to improving the quality, performance, or usability of pre-release versions of Your Application (e.g., continuous distribution of demo versions of Your Application in an attempt to circumvent the App Store or providing trial versions of Your Applications for purposes of soliciting favorable App Store ratings are prohibited uses). Further, if Your Application is primarily intended for children, You must verify that Your Beta Testers are of the age of majority in their jurisdiction. If You choose to add Beta Testers to TestFlight, then You are assuming responsibility for any invitations sent to such end-users and for obtaining their consent to contact them. Apple will use the email addresses that You provide through TestFlight only for purposes of sending invitations to such end-users via TestFlight. By uploading email addresses for the purposes of sending invites to Beta Testers, You warrant that You have an appropriate legal basis for using such emails addresses for the purposes of sending invites. If a Beta Tester requests that You stop contacting them (either through TestFlight or otherwise), then You agree to promptly do so.

C. Use of TestFlight Information

To the extent that TestFlight provides You with beta analytics information about Your end-user's use of pre-release versions of Your Application (e.g., installation time, frequency of an individual's use of an App, etc.) and/or other related information (e.g. tester suggestions, feedback, screenshots), You agree to use such data solely for purposes of improving Your Applications and related products. You agree not to provide such information to any third parties, except for a Service Provider who is assisting You in processing and analyzing such data on Your behalf and who is not permitted to use it for any other purpose or disclose it to any other party (and then only to the limited extent not prohibited by Apple). For clarity, You must not aggregate (or permit any third-party to aggregate) beta analytics information provided to You by Apple for Your Applications as part of TestFlight with other developers' beta analytics information, or contribute such information to a repository for cross-developer beta analytics information. Further, You must not use any beta analytics information provided through TestFlight for purposes of de-anonymizing information obtained from or regarding a particular device or end-user outside of TestFlight (e.g., You may not attempt to connect data gathered through TestFlight for a particular end-user with information that is provided in an anonymized form through Apple's analytics service).

Libraries:

7.5 Distribution of Libraries

You can develop Libraries using the Apple Software. Notwithstanding anything to the contrary in the Xcode and Apple SDKs Agreement, under this Agreement You may develop Libraries for iOS, watchOS, iPadOS, and tvOS using the applicable Apple SDKs that are provided as part of the Xcode and Apple SDKs license, provided that any such Libraries are developed and distributed solely for use with an iOS Product, Apple Watch, or Apple TV and that You limit use of such Libraries only to use with such products. If Apple determines that Your Library is not designed for use with an iOS Product, Apple Watch, or Apple TV, then Apple may require You to cease distribution of Your Library at any time, and You agree to promptly cease all distribution of such Library upon notice from Apple and cooperate with Apple to remove any remaining copies of such Library. For clarity, the foregoing limitation is not intended to prohibit the development of libraries for macOS.

7.6 No Other Distribution Authorized Under this Agreement

Except for the distribution of freely available Licensed Applications through the App Store or Custom App Distribution in accordance with **Sections 7.1** and **7.2**, the distribution of Applications for use on Registered Devices as set forth in **Section 7.2** (Ad Hoc Distribution), the distribution of Applications for beta testing through TestFlight as set forth in **Section 7.4**, the distribution of Libraries in accordance with **Section 7.5**, the distribution of Passes in accordance with Attachment 5, the delivery of Safari Push Notifications on macOS, the distribution of Safari Extensions on macOS, the distribution of Applications and libraries developed for macOS, and/or as otherwise permitted herein, no other distribution of programs or applications developed using the Apple Software is authorized or permitted hereunder. In the absence of a separate agreement with Apple, You agree not to distribute Your Application for iOS Products, Apple Watch, or Apple TV to third parties via other distribution methods or to enable or permit others to do so. You agree to distribute Your Covered Products only in accordance with the terms of this Agreement.

8. Program Fees

As consideration for the rights and licenses granted to You under this Agreement and Your participation in the Program, You agree to pay Apple the annual Program fee set forth on the Program website, unless You have received a valid fee waiver from Apple. Such fee is non-refundable, and any taxes that may be levied on the Apple Software, Apple Services or Your use of the Program shall be Your responsibility. Your Program fees must be paid up and not in

arrears at the time You submit (or resubmit) Applications to Apple under this Agreement, and Your continued use of the Program web portal and Services is subject to Your payment of such fees, where applicable. If You opt-in to have Your annual Program fees paid on an auto-renewing basis, then You agree that Apple may charge the credit card that You have on file with Apple for such fees, subject to the terms You agree to on the Program web portal when You choose to enroll in an auto-renewing membership.

9. Confidentiality

9.1 Information Deemed Apple Confidential

You agree that all pre-release versions of the Apple Software and Apple Services (including pre-release Documentation), pre-release versions of Apple hardware, the FPS Deployment Package, any terms and conditions contained herein that disclose pre-release features, and the terms and conditions of Schedule 2 and Schedule 3 will be deemed "Apple Confidential Information"; provided however that upon the commercial release of the Apple Software the terms and conditions that disclose pre-release features of the Apple Software or services will no longer be confidential. Notwithstanding the foregoing, Apple Confidential Information will not include: (i) information that is generally and legitimately available to the public through no fault or breach of Yours, (ii) information that is generally made available to the public by Apple, (iii) information that is independently developed by You without the use of any Apple Confidential Information, (iv) information that was rightfully obtained from a third party who had the right to transfer or disclose it to You without limitation, or (v) any FOSS included in the Apple Software and accompanied by licensing terms that do not impose confidentiality obligations on the use or disclosure of such FOSS. Further, Apple agrees that You will not be bound by the foregoing confidentiality terms with regard to technical information about pre-release Apple Software and services disclosed by Apple at WWDC (Apple's Worldwide Developers Conference), except that You may not post screen shots of, write public reviews of, or redistribute any pre-release Apple Software, Apple Services or hardware.

9.2 Obligations Regarding Apple Confidential Information

You agree to protect Apple Confidential Information using at least the same degree of care that You use to protect Your own confidential information of similar importance, but no less than a reasonable degree of care. You agree to use Apple Confidential Information solely for the purpose of exercising Your rights and performing Your obligations under this Agreement and agree not to use Apple Confidential Information for any other purpose, for Your own or any third party's benefit, without Apple's prior written consent. You further agree not to disclose or disseminate Apple Confidential Information to anyone other than: (i) those of Your employees and contractors, or those of Your faculty and staff if You are an educational institution, who have a need to know and who are bound by a written agreement that prohibits unauthorized use or disclosure of the Apple Confidential Information; or (ii) except as otherwise agreed or permitted in writing by Apple. You may disclose Apple Confidential Information to the extent required by law, provided that You take reasonable steps to notify Apple of such requirement before disclosing the Apple Confidential Information and to obtain protective treatment of the Apple Confidential Information. You acknowledge that damages for improper disclosure of Apple Confidential Information may be irreparable; therefore, Apple is entitled to seek equitable relief, including injunction and preliminary injunction, in addition to all other remedies.

9.3 Information Submitted to Apple Not Deemed Confidential

Apple works with many application and software developers and some of their products may be similar to or compete with Your Applications. Apple may also be developing its own similar or competing applications and products or may decide to do so in the future. To avoid potential misunderstandings and except as otherwise expressly set forth herein, Apple cannot agree, and expressly disclaims, any confidentiality obligations or use restrictions, express or implied, with respect to any information that You may provide in connection with this Agreement or the Program, including but not limited to information about Your Application, Licensed Application Information, and metadata (such disclosures will be referred to as "**Licensee Disclosures**"). You

agree that any such Licensee Disclosures will be **non-confidential**. Except as otherwise expressly set forth herein, Apple will be free to use and disclose any Licensee Disclosures on an unrestricted basis without notifying or compensating You. You release Apple from all liability and obligations that may arise from the receipt, review, use, or disclosure of any portion of any Licensee Disclosures. Any physical materials You submit to Apple will become Apple property and Apple will have no obligation to return those materials to You or to certify their destruction.

9.4 Press Releases and Other Publicity

You may not issue any press releases or make any other public statements regarding this Agreement, its terms and conditions, or the relationship of the parties without Apple's express prior written approval, which may be withheld at Apple's discretion.

10. Indemnification

To the extent permitted by applicable law, You agree to indemnify and hold harmless, and upon Apple's request, defend, Apple, its directors, officers, employees, independent contractors and agents (each an "Apple Indemnified Party") from any and all claims, losses, liabilities, damages, taxes, expenses and costs, including without limitation, attorneys' fees and court costs (collectively, "Losses"), incurred by an Apple Indemnified Party and arising from or related to any of the following (but excluding for purposes of this Section, any Application for macOS that is distributed outside of the App Store and does not use any Apple Services or Certificates): (i) Your breach of any certification, covenant, obligation, representation or warranty in this Agreement, including Schedule 2 and Schedule 3 (if applicable); (ii) any claims that Your Covered Product or the distribution, sale, offer for sale, use or importation of Your Covered Product (whether alone or as an essential part of a combination), Licensed Application Information, metadata, or Pass Information violate or infringe any third party intellectual property or proprietary rights; (iii) Your breach of any of Your obligations under the EULA (as defined in Schedule 1 or Schedule 2 or Schedule 3 (if applicable)) for Your Licensed Application; (iv) Apple's permitted use, promotion or delivery of Your Licensed Application, Licensed Application Information, Safari Push Notification, Safari Extension (if applicable), Pass, Pass Information, metadata, related trademarks and logos, or images and other materials that You provide to Apple under this Agreement, including Schedule 2 or Schedule 3 (if applicable); (v) any claims, including but not limited to any end-user claims, regarding Your Covered Products, Licensed Application Information, Pass Information, or related logos, trademarks, content or images; or (vi) Your use (including Your Authorized Developers' use) of the Apple Software or services, Your Licensed Application Information, Pass Information, metadata, Your Authorized Test Units, Your Registered Devices, Your Covered Products, or Your development and distribution of any of the foregoing.

You acknowledge that neither the Apple Software nor any Services are intended for use in the development of Covered Products in which errors or inaccuracies in the content, functionality, services, data or information provided by any of the foregoing or the failure of any of the foregoing, could lead to death, personal injury, or severe physical or environmental damage, and, to the extent permitted by law, You hereby agree to indemnify, defend and hold harmless each Apple Indemnified Party from any Losses incurred by such Apple Indemnified Party by reason of any such use.

In no event may You enter into any settlement or like agreement with a third party that affects Apple's rights or binds Apple in any way, without the prior written consent of Apple.

11. Term and Termination

11.1 Term

The Term of this Agreement shall extend until the one (1) year anniversary of the original activation date of Your Program account. Thereafter, subject to Your payment of annual renewal fees and compliance with the terms of this Agreement, the Term will automatically renew for successive one (1) year terms, unless sooner terminated in accordance with this Agreement.

11.2 Termination

This Agreement and all rights and licenses granted by Apple hereunder and any services provided hereunder will terminate, effective immediately upon notice from Apple:
(a) if You or any of Your Authorized Developers fail to comply with any term of this Agreement other than those set forth below in this **Section 11.2** and fail to cure such breach within 30 days after becoming aware of or receiving notice of such breach;
(b) if You or any of Your Authorized Developers fail to comply with the terms of **Section 9 (Confidentiality)**;
(c) in the event of the circumstances described in the subsection entitled "Severability" below;
(d) if You, at any time during the Term, commence an action for patent infringement against Apple;
(e) if You become insolvent, fail to pay Your debts when due, dissolve or cease to do business, file for bankruptcy, or have filed against You a petition in bankruptcy; or
(f) if You engage, or encourage others to engage, in any misleading, fraudulent, improper, unlawful or dishonest act relating to this Agreement, including, but not limited to, misrepresenting the nature of Your submitted Application (e.g., hiding or trying to hide functionality from Apple's review, falsifying consumer reviews for Your Application, engaging in payment fraud, etc.).

Apple may also terminate this Agreement, or suspend Your rights to use the Apple Software or services, if You fail to accept any new Program Requirements or Agreement terms as described in **Section 4**. Either party may terminate this Agreement for its convenience, for any reason or no reason, effective 30 days after providing the other party with written notice of its intent to terminate.

11.3 Effect of Termination

Upon the termination of this Agreement for any reason, You agree to immediately cease all use of the Apple Software and services and erase and destroy all copies, full or partial, of the Apple Software and any information pertaining to the services (including Your Push Application ID) and all copies of Apple Confidential Information in Your and Your Authorized Developers' possession or control. At Apple's request, You agree to provide written certification of such destruction to Apple. Upon the expiration of the Delivery Period defined and set forth in Schedule 1, all Licensed Applications and Licensed Application Information in Apple's possession or control shall be deleted or destroyed within a reasonable time thereafter, excluding any archival copies maintained in accordance with Apple's standard business practices or required to be maintained by applicable law, rule or regulation. The following provisions shall survive any termination of this Agreement: Sections 1, 2.3, 2.5, 2.6, 3.1(d), 3.1(e), 3.1(f), 3.2(d), 3.2(e), 3.2(f), 3.2(g), and 3.3, the second paragraph of Section 5.1 (excluding the last two sentences other than the restrictions, which shall survive), the third paragraph of Section 5.1, the last sentence of the first paragraph of Section 5.3 and the limitations and restrictions of Section 5.3, Section 5.4, the first sentence of and the restrictions of Section 6.6, the restrictions of Section 6.7, the second paragraph of Section 6.9, Section 7.1 (Schedule 1 for the Delivery Period), the restrictions of Section 7.3, 7.4, and 7.5, Section 7.6, Section 9 through14 inclusive; within Attachment 1, the last sentence of Section 1.1, Section 2, Section 3.2 (but only for existing promotions), the second and third sentences of Section 4, Section 5, and Section 6; within Attachment 2, Sections 1.3, 2, 3, 4, 5, 6, and 7; within Attachment 3, Sections 1, 2 (except the second sentence of Section 2.1), 3 and 4; within Attachment 4, Sections 1.2, 1.5, 1.6, 2, 3, and 4; within Attachment 5, Sections 2.2, 2.3, 2.4 (but only for existing promotions), 3.3, and 5; within Attachment 6, Sections 1.2, 1.3, 2, 3, and 4; and within Attachment 7, Section 1.1 and Section 1.2. Apple will not be liable for compensation, indemnity, or damages of any sort as a result of terminating this Agreement in accordance with its terms, and termination of this Agreement will be without prejudice to any other right or remedy Apple may have, now or in the future.

12. NO WARRANTY

The Apple Software or Services may contain inaccuracies or errors that could cause failures or loss of data and it may be incomplete. Apple and its licensors reserve the right to change,

suspend, remove, or disable access to any Services (or any part thereof) at any time without notice. In no event will Apple or its licensors be liable for the removal of or disabling of access to any such Services. Apple or its licensors may also impose limits on the use of or access to certain Services, or may remove the Services for indefinite time periods or cancel the Services at any time and in any case and without notice or liability. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, YOU EXPRESSLY ACKNOWLEDGE AND AGREE THAT USE OF THE APPLE SOFTWARE, SECURITY SOLUTION, AND ANY SERVICES IS AT YOUR SOLE RISK AND THAT THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH YOU. THE APPLE SOFTWARE, SECURITY SOLUTION, AND ANY SERVICES ARE PROVIDED “AS IS” AND “AS AVAILABLE”, WITH ALL FAULTS AND WITHOUT WARRANTY OF ANY KIND, AND APPLE, APPLE’S AGENTS AND APPLE'S LICENSORS (**COLLECTIVELY REFERRED TO AS “APPLE” FOR THE PURPOSES OF SECTIONS 12 AND 13**) HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH RESPECT TO THE APPLE SOFTWARE, SECURITY SOLUTION, AND SERVICES, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, TIMELINESS, AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS. APPLE DOES NOT WARRANT AGAINST INTERFERENCE WITH YOUR ENJOYMENT OF THE APPLE SOFTWARE, SECURITY SOLUTION, OR SERVICES, THAT THE APPLE SOFTWARE, SECURITY SOLUTION, OR SERVICES WILL MEET YOUR REQUIREMENTS, THAT THE OPERATION OF THE APPLE SOFTWARE, SECURITY SOLUTION, OR THE PROVISION OF SERVICES WILL BE UNINTERRUPTED, TIMELY, SECURE OR ERROR-FREE, THAT DEFECTS OR ERRORS IN THE APPLE SOFTWARE, SECURITY SOLUTION, OR SERVICES WILL BE CORRECTED, OR THAT THE APPLE SOFTWARE, SECURITY SOLUTION, OR SERVICES WILL BE COMPATIBLE WITH FUTURE APPLE PRODUCTS, SERVICES OR SOFTWARE OR ANY THIRD PARTY SOFTWARE, APPLICATIONS, OR SERVICES, OR THAT ANY INFORMATION STORED OR TRANSMITTED THROUGH ANY APPLE SOFTWARE OR SERVICES WILL NOT BE LOST, CORRUPTED OR DAMAGED. YOU ACKNOWLEDGE THAT THE APPLE SOFTWARE AND SERVICES ARE NOT INTENDED OR SUITABLE FOR USE IN SITUATIONS OR ENVIRONMENTS WHERE ERRORS, DELAYS, FAILURES OR INACCURACIES IN THE TRANSMISSION OR STORAGE OF DATA OR INFORMATION BY OR THROUGH THE APPLE SOFTWARE OR SERVICES COULD LEAD TO DEATH, PERSONAL INJURY, OR FINANCIAL, PHYSICAL, PROPERTY OR ENVIRONMENTAL DAMAGE, INCLUDING WITHOUT LIMITATION THE OPERATION OF NUCLEAR FACILITIES, AIRCRAFT NAVIGATION OR COMMUNICATION SYSTEMS, AIR TRAFFIC CONTROL, LIFE SUPPORT OR WEAPONS SYSTEMS. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY APPLE OR AN APPLE AUTHORIZED REPRESENTATIVE WILL CREATE A WARRANTY NOT EXPRESSLY STATED IN THIS AGREEMENT. SHOULD THE APPLE SOFTWARE, SECURITY SOLUTION, OR SERVICES PROVE DEFECTIVE, YOU ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. Location data as well as any maps data provided by any Services or software is for basic navigational purposes only and is not intended to be relied upon in situations where precise location information is needed or where erroneous, inaccurate or incomplete location data may lead to death, personal injury, property or environmental damage. Neither Apple nor any of its licensors guarantees the availability, accuracy, completeness, reliability, or timeliness of location data or any other data or information displayed by any Services or software.

13. LIMITATION OF LIABILITY

TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT WILL APPLE BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT, CONSEQUENTIAL OR PUNITIVE DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, LOSS OF DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO THIS AGREEMENT, YOUR USE OR INABILITY TO USE THE APPLE

SOFTWARE, SECURITY SOLUTION, SERVICES, APPLE CERTIFICATES, OR YOUR DEVELOPMENT EFFORTS OR PARTICIPATION IN THE PROGRAM, HOWEVER CAUSED, WHETHER UNDER A THEORY OF CONTRACT, WARRANTY, TORT (INCLUDING NEGLIGENCE), PRODUCTS LIABILITY, OR OTHERWISE, EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY. In no event shall Apple's total liability to You under this Agreement for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of fifty dollars ($50.00).

14. General Legal Terms

14.1 Third Party Notices

Portions of the Apple Software or Services may utilize or include third party software and other copyrighted material. Acknowledgements, licensing terms and disclaimers for such material are contained in the electronic documentation for the Apple Software and Services, and Your use of such material is governed by their respective terms.

14.2 Consent to Collection and Use of Data

A. Pre-Release Versions of iOS, watchOS, tvOS, iPadOS, and macOS

In order to provide, test and help Apple, its partners, and third party developers improve their products and services, and unless You or Your Authorized Developers opt out in the pre-release versions of iOS, watchOS, tvOS, iPadOS, or macOS, as applicable, You acknowledge that Apple and its subsidiaries and agents will be collecting, using, storing, transmitting, processing and analyzing (collectively, "**Collecting**") diagnostic, technical, and usage logs and information from Your Authorized Test Units (that are running pre-release versions of the Apple Software and services) as part of the developer seeding process. This information will be Collected in a form that does not personally identify You or Your Authorized Developers and may be Collected from Your Authorized Test Units at any time. The information that would be Collected includes, but is not limited to, general diagnostic and usage data, various unique device identifiers, various unique system or hardware identifiers, details about hardware and operating system specifications, performance statistics, and data about how You use Your Authorized Test Unit, system and application software, and peripherals, and, if Location Services is enabled, certain location information. You agree that Apple may share such diagnostic, technical, and usage logs and information with partners and third-party developers for purposes of allowing them to improve their products and services that operate on or in connection with Apple-branded products. **By installing or using pre-release versions of iOS, watchOS, tvOS, iPadOS, or macOS on Your Authorized Test Units, You acknowledge and agree that Apple and its subsidiaries and agents have Your permission to Collect all such information and use it as set forth above in this Section.**

B. Other Pre-Release Apple Software and Services

In order to test, provide and improve Apple's products and services, and only if You choose to install or use other pre-release Apple Software or Services provided as part of the developer seeding process or Program, You acknowledge that Apple and its subsidiaries and agents may be Collecting diagnostic, technical, usage and related information from other pre-release Apple Software and Services. Apple will notify You about the Collection of such information on the Program web portal, and You should carefully review the release notes and other information disclosed by Apple in such location prior to choosing whether or not to install or use any such pre-release Apple Software or Services. **By installing or using such pre-release Apple Software and Services, You acknowledge and agree that Apple and its subsidiaries and agents have Your permission to Collect any and all such information and use it as set forth above.**

C. Device Deployment Services

In order to set up and use the device provisioning, account authentication, and deployment features of the Apple Software and Services, certain unique identifiers for Your computer, iOS Products, watchOS devices, tvOS devices, and account information may be needed. These

unique identifiers may include Your email address, Your Apple ID, a hardware identifier for Your computer, and device identifiers entered by You into the Apple Software or Services for such Apple-branded products. Such identifiers may be logged in association with Your interaction with the Service and Your use of these features and the Apple Software and Services. **By using these features, You agree that Apple and its subsidiaries and agents may Collect this information for the purpose of providing the Apple Software and Services, including using such identifiers for account verification and anti-fraud measures.** If You do not want to provide this information, do not use the provisioning, deployment or authentication features of the Apple Software or Services.

D. Apple Services

In order to test, provide and improve Apple's products and services, and only if You choose to use the Services provided hereunder (and except as otherwise provided herein), You acknowledge that Apple and its subsidiaries and agents may be Collecting diagnostic, technical, usage and related information from the Apple Services. Some of this information will be Collected in a form that does not personally identify You. However, in some cases, Apple may need to Collect information that would personally identify You, but only if Apple has a good faith belief that such Collection is reasonably necessary to: (a) provide the Apple Services; (b) comply with legal process or request; (c) verify compliance with the terms of this Agreement; (d) prevent fraud, including investigating any potential technical issues or violations; or (e) protect the rights, property, security or safety of Apple, its developers, customers or the public as required or permitted by law. **By installing or using such Apple Services, You acknowledge and agree that Apple and its subsidiaries and agents have Your permission to Collect any and all such information and use it as set forth in this Section.** Further, You agree that Apple may share the diagnostic, technical, and usage logs and information (excluding personally identifiable information) with partners and third-party developers for purposes of allowing them to improve their products and services that operate on or in connection with Apple-branded products.

E. Privacy Policy

Data collected pursuant to this **Section 14.2** will be treated in accordance with Apple's Privacy Policy which can be viewed at http://www.apple.com/legal/privacy.

14.3 Assignment; Relationship of the Parties

This Agreement may not be assigned, nor may any of Your obligations under this Agreement be delegated, in whole or in part, by You by operation of law, merger, or any other means without Apple's express prior written consent and any attempted assignment without such consent will be null and void. To submit a request for Apple's consent to assignment, please email devprograms@apple.com, or, notwithstanding **Section 14.5**, send a written request to Developer Relations Customer Support, 1 Infinite Loop MS 301-1TEV Cupertino, CA, USA 95014. Except for the agency appointment as specifically set forth in Schedule 1 (if applicable), this Agreement will not be construed as creating any other agency relationship, or a partnership, joint venture, fiduciary duty, or any other form of legal association between You and Apple, and You will not represent to the contrary, whether expressly, by implication, appearance or otherwise. This Agreement is not for the benefit of any third parties.

14.4 Independent Development

Nothing in this Agreement will impair Apple's right to develop, acquire, license, market, promote, or distribute products or technologies that perform the same or similar functions as, or otherwise compete with, Licensed Applications, Covered Products, or any other products or technologies that You may develop, produce, market, or distribute.

14.5 Notices

Any notices relating to this Agreement shall be in writing, except as otherwise set forth in **Section 14.3**. Notices will be deemed given by Apple when sent to You at the email address or mailing address You provided during the sign-up process. Except as set forth in **Section 14.3**, all notices to Apple relating to this Agreement will be deemed given (a) when delivered personally, (b) three

business days after having been sent by commercial overnight carrier with written proof of delivery, and (c) five business days after having been sent by first class or certified mail, postage prepaid, to this Apple address: Apple Developer Program Licensing, Apple Inc., App Store Legal, One Apple Park Way, 169-4ISM, Cupertino, California, 95014 U.S.A. You consent to receive notices by email and agree that any such notices that Apple sends You electronically will satisfy any legal communication requirements. A party may change its email or mailing address by giving the other written notice as described above.

14.6 Severability

If a court of competent jurisdiction finds any clause of this Agreement to be unenforceable for any reason, that clause of this Agreement shall be enforced to the maximum extent permissible so as to effect the intent of the parties, and the remainder of this Agreement shall continue in full force and effect. However, if applicable law prohibits or restricts You from fully and specifically complying with, or appointing Apple and Apple Subsidiaries as Your agent under Schedule 1 or the Sections of this Agreement entitled “Internal Use License and Restrictions”, “Your Obligations” or “Apple Certificates; Revocation”, or prevents the enforceability of any of those Sections or Schedule 1, this Agreement will immediately terminate and You must immediately discontinue any use of the Apple Software as described in the Section entitled “Term and Termination.”

14.7 Waiver and Construction

Failure by Apple to enforce any provision of this Agreement shall not be deemed a waiver of future enforcement of that or any other provision. Any laws or regulations that provide that the language of a contract will be construed against the drafter will not apply to this Agreement. Section headings are for convenience only and are not to be considered in construing or interpreting this Agreement.

14.8 Export Control

You may not use, export, re-export, import, sell, release, or transfer the Apple Software, Services, or Documentation except as authorized by United States law, the laws of the jurisdiction in which You obtained the Apple Software, and any other applicable laws and regulations. In particular, but without limitation, the Apple Software, Services, and Documentation may not be exported, or re-exported, transferred, or released (a) into any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department’s list of Specially Designated Nationals or the U.S. Department of Commerce’s Denied Persons List or Entity List or any other restricted party lists. By using the Apple Software, Services, or Documentation, You represent and warrant that You are not located in any such country or on any such list. You also agree that You will not use the Apple Software, Services, or Documentation for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture or production of nuclear, missile, chemical or biological weapons. You certify that pre-release versions of the Apple Software, Services or Documentation will only be used for development and testing purposes, and will not be rented, sold, leased, sublicensed, assigned, or otherwise transferred. Further, You certify that You will not transfer or export any product, process or service that is a direct product of such pre-release Apple Software, Services, or Documentation.

14.9 Government End-users

The Apple Software and Documentation are “Commercial Items”, as that term is defined at 48 C.F.R. §2.101, consisting of “Commercial Computer Software” and “Commercial Computer Software Documentation”, as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end-users (a) only as Commercial Items and (b) with only those rights as are granted to all other end-users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

14.10 Dispute Resolution; Governing Law

Any litigation or other dispute resolution between You and Apple arising out of or relating to this Agreement, the Apple Software, or Your relationship with Apple will take place in the Northern District of California, and You and Apple hereby consent to the personal jurisdiction of and exclusive venue in the state and federal courts within that District with respect any such litigation or dispute resolution. This Agreement will be governed by and construed in accordance with the laws of the United States and the State of California, except that body of California law concerning conflicts of law. Notwithstanding the foregoing:

(a) If You are an agency, instrumentality or department of the federal government of the United States, then this Agreement shall be governed in accordance with the laws of the United States of America, and in the absence of applicable federal law, the laws of the State of California will apply. Further, and notwithstanding anything to the contrary in this Agreement (including but not limited to **Section 10 (Indemnification)**), all claims, demands, complaints and disputes will be subject to the Contract Disputes Act (41 U.S.C. §§601-613), the Tucker Act (28 U.S.C. § 1346(a) and § 1491), or the Federal Tort Claims Act (28 U.S.C. §§ 1346(b), 2401-2402, 2671-2672, 2674-2680), as applicable, or other applicable governing authority. For the avoidance of doubt, if You are an agency, instrumentality, or department of the federal, state or local government of the U.S. or a U.S. public and accredited educational institution, then Your indemnification obligations are only applicable to the extent they would not cause You to violate any applicable law (e.g., the Anti-Deficiency Act), and You have any legally required authorization or authorizing statute;
(b) If You (as an entity entering into this Agreement) are a U.S. public and accredited educational institution or an agency, instrumentality, or department of a state or local government within the United States, then (a) this Agreement will be governed and construed in accordance with the laws of the state (within the U.S.) in which Your entity is domiciled, except that body of state law concerning conflicts of law; and (b) any litigation or other dispute resolution between You and Apple arising out of or relating to this Agreement, the Apple Software, or Your relationship with Apple will take place in federal court within the Northern District of California, and You and Apple hereby consent to the personal jurisdiction of and exclusive venue of such District unless such consent is expressly prohibited by the laws of the state in which Your entity is domiciled; and
(c) If You are an international, intergovernmental organization that has been conferred immunity from the jurisdiction of national courts through Your intergovernmental charter or agreement, then any controversy or claim arising out of or relating to this Agreement, or the breach thereof, shall be determined by arbitration administered by the International Centre for Dispute Resolution in accordance with its International Arbitration Rules. The place of arbitration shall be London, England; the language shall be English; and the number of arbitrators shall be three. Upon Apple's request, You agree to provide evidence of Your status as an intergovernmental organization with such privileges and immunities.

This Agreement shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

14.11 Entire Agreement; Governing Language

This Agreement constitutes the entire agreement between the parties with respect to the use of the Apple Software, Apple Services and Apple Certificates licensed hereunder and, except as otherwise set forth herein, supersedes all prior understandings and agreements regarding its subject matter. Notwithstanding the foregoing, to the extent that You are provided with pre-release materials under the Program and such pre-release materials are subject to a separate license agreement, You agree that the license agreement accompanying such materials in addition to **Section 9 (Confidentiality)** of this Agreement shall also govern Your use of such materials. If You have entered or later enter into the Xcode and Apple SDKs Agreement, this Apple Developer Program License Agreement will govern in the event of any inconsistencies between the two with respect to the same subject matter; provided, however, that this Apple Developer Program License Agreement is not intended to prevent You from exercising any rights granted to You in the Xcode and Apple SDKs Agreement in accordance with the terms and conditions set forth therein. This Agreement may be modified only: (a) by a written amendment signed by both parties, or (b) to the extent expressly permitted by this Agreement (for example,

by Apple by written or email notice to You). Any translation is provided as a courtesy to You, and in the event of a dispute between the English and any non-English version, the English version of this Agreement shall govern, to the extent not prohibited by local law in Your jurisdiction. If You are located in the province of Quebec, Canada or are a government organization within France, then the following clause applies to You: The parties hereby confirm that they have requested that this Agreement and all related documents be drafted in English. *Les parties ont exigé que le présent contrat et tous les documents connexes soient rédigés en anglais.*

Attachment 1
(to the Agreement)
Additional Terms for Apple Push Notification Service and Local Notifications

The following terms are in addition to the terms of the Agreement and apply to any use of the APN (Apple Push Notification Service):

1. Use of the APN and Local Notifications

1.1 You may use the APN only in Your Applications, Your Passes, and/or in sending Safari Push Notifications to the macOS desktop of users of Your Site who have opted in to receive Notifications through Safari on macOS. You, Your Application and/or Your Pass may access the APN only via the APN API and only if You have been assigned a Push Application ID by Apple. Except for a Service Provider who is assisting You with using the APN, You agree not to share Your Push Application ID with any third party. You understand that You will not be permitted to access or use the APN after expiration or termination of Your Agreement.

1.2 You are permitted to use the APN and the APN APIs only for the purpose of sending Push Notifications to Your Application, Your Pass, and/or to the macOS desktop of users of Your Site who have opted in to receive Notifications through Safari on macOS as expressly permitted by the Agreement, the APN Documentation and all applicable laws and regulations (including all intellectual property laws). You further agree that You must disclose to Apple any use of the APN as part of the submission process for Your Application.

1.3 You understand that before You send an end-user any Push Notifications through the APN, the end-user must consent to receive such Notifications. You agree not to disable, override or otherwise interfere with any Apple-implemented consent panels or any Apple system preferences for enabling or disabling Notification functionality. If the end-user's consent to receive Push Notifications is denied or later withdrawn, You may not send the end-user Push Notifications.

2. Additional Requirements

2.1 You may not use the APN or Local Notifications for the purpose of sending unsolicited messages to end-users or for the purpose of phishing or spamming, including, but not limited to, engaging in any types of activities that violate anti-spamming laws and regulations, or that are otherwise improper, inappropriate or illegal. The APN and Local Notifications should be used for sending relevant messages to a user that provide a benefit (e.g., a response to an end-user request for information, provision of pertinent information relevant to the Application).

2.2 You may not use the APN or Local Notifications for the purposes of advertising, product promotion, or direct marketing of any kind (e.g., up-selling, cross-selling, etc.), including, but not limited to, sending any messages to promote the use of Your Application or advertise the availability of new features or versions. Notwithstanding the foregoing, You may use the APN or Local Notifications for promotional purposes in connection with Your Pass so long as such use is directly related to the Pass, e.g., a store coupon may be sent to Your Pass in Wallet.

2.3 You may not excessively use the overall network capacity or bandwidth of the APN, or unduly burden an iOS Product, Apple Watch, macOS or an end-user with excessive Push Notifications or Local Notifications, as may be determined by Apple in its reasonable discretion. In addition, You agree not to harm or interfere with Apple's networks or servers, or any third party servers or networks connected to the APN, or otherwise disrupt other developers' use of the APN.

2.4 You may not use the APN or Local Notifications to send material that contains any obscene, pornographic, offensive or defamatory content or materials of any kind (text, graphics,

images, photographs, sounds, etc.), or other content or materials that in Apple's reasonable judgment may be found objectionable by the end-user of Your Application, Pass or Site.

2.5 You may not transmit, store or otherwise make available any material that contains viruses or any other computer code, files or programs that may harm, disrupt or limit the normal operation of the APN or an iOS Product, Apple Watch, or macOS, and You agree not to disable, spoof, hack or otherwise interfere with any security, digital signing, verification or authentication mechanisms that are incorporated in or used by the APN, or enable others to do so.

3. Additional Terms for Website Push IDs

3.1 Subject to the terms of this Agreement, You understand and agree that Safari Push Notifications that You send using Your Website Push ID must be sent under Your own name, trademark or brand (e.g., a user should know that the communication is coming from Your Site) and must include an icon, trademark, logo or other identifying mark for Your Site. You agree not to misrepresent or impersonate another Site or entity or otherwise mislead users about the originator of the Safari Push Notification. To the extent that You reference a third party's trademark or brand within Your Safari Push Notification, You represent and warrant that You have any necessary rights.

3.2 By enabling the APN and sending Safari Push Notifications for Your Site as permitted in this Agreement, You hereby permit Apple to use (i) screen shots of Your Safari Push Notifications on macOS; and (ii) trademarks and logos associated with such Notifications, for promotional purposes in Apple's marketing materials, excluding those portions which You do not have the right to use for promotional purposes and which You identify in writing to Apple. You also permit Apple to use images and other materials that You may provide to Apple, at Apple's reasonable request, for promotional purposes in marketing materials.

4. Delivery by the APN or via Local Notifications. You understand and agree that in order to provide the APN and make Your Push Notifications available on iOS Products, Apple Watch, or macOS, Apple may transmit Your Push Notifications across various public networks, in various media, and modify or change Your Push Notifications to comply with the technical and other requirements for connecting to networks or devices. You acknowledge and agree that the APN is not, and is not intended to be, a guaranteed or secure delivery service, and You shall not use or rely upon it as such. Further, as a condition to using the APN or delivering Local Notifications, You agree not to transmit sensitive personal or confidential information belonging to an individual (e.g., a social security number, financial account or transactional information, or any information where the individual may have a reasonable expectation of secure transmission) as part of any such Notification, and You agree to comply with any applicable notice or consent requirements with respect to any collection, transmission, maintenance, processing or use of an end-user's personal information.

5. Your Acknowledgements. You acknowledge and agree that:

5.1 Apple may at any time, and from time to time, with or without prior notice to You (a) modify the APN, including changing or removing any feature or functionality, or (b) modify, deprecate, reissue or republish the APN APIs. You understand that any such modifications may require You to change or update Your Applications, Passes or Sites at Your own cost. Apple has no express or implied obligation to provide, or continue to provide, the APN and may suspend or discontinue all or any portion of the APN at any time. Apple shall not be liable for any losses, damages or costs of any kind incurred by You or any other party arising out of or related to any such service suspension or discontinuation or any such modification of the APN or APN APIs.

5.2 The APN is not available in all languages or in all countries and Apple makes no representation that the APN is appropriate or available for use in any particular location. To the

extent You choose to access and use the APN, You do so at Your own initiative and are responsible for compliance with any applicable laws, including but not limited to any local laws.

5.3 Apple provides the APN to You for Your use with Your Application, Pass, or Site, and does not provide the APN directly to any end-user. You acknowledge and agree that any Push Notifications are sent by You, not Apple, to the end-user of Your Application, Pass or Site, and You are solely liable and responsible for any data or content transmitted therein and for any such use of the APN. Further, You acknowledge and agree that any Local Notifications are sent by You, not Apple, to the end-user of Your Application, and You are solely liable and responsible for any data or content transmitted therein.

5.4 Apple makes no guarantees to You in relation to the availability or uptime of the APN and is not obligated to provide any maintenance, technical or other support for the APN.

5.5 Apple reserves the right to remove Your access to the APN, limit Your use of the APN, or revoke Your Push Application ID at any time in its sole discretion.

5.6 Apple may monitor and collect information (including but not limited to technical and diagnostic information) about Your usage of the APN to aid Apple in improving the APN and other Apple products or services and to verify Your compliance with this Agreement; provided however that Apple will not access or disclose the content of any Push Notification unless Apple has a good faith belief that such access or disclosure is reasonably necessary to: (a) comply with legal process or request; (b) enforce the terms of this Agreement, including investigation of any potential violation hereof; (c) detect, prevent or otherwise address security, fraud or technical issues; or (d) protect the rights, property or safety of Apple, its developers, customers or the public as required or permitted by law. Notwithstanding the foregoing, You acknowledge and agree that iOS, iPadOS, macOS, and watchOS may access Push Notifications locally on a user's device solely for the purposes of responding to user requests and personalizing user experience and suggestions on device.

6. Additional Liability Disclaimer. APPLE SHALL NOT BE LIABLE FOR ANY DAMAGES OR LOSSES ARISING FROM ANY USE OF THE APN, INCLUDING ANY INTERRUPTIONS TO THE APN OR ANY USE OF NOTIFICATIONS, INCLUDING, BUT NOT LIMITED TO, ANY POWER OUTAGES, SYSTEM FAILURES, NETWORK ATTACKS, SCHEDULED OR UNSCHEDULED MAINTENANCE, OR OTHER INTERRUPTIONS.

Attachment 2
(to the Agreement)
Additional Terms for Use of the In-App Purchase API

The following terms are in addition to the terms of the Agreement and apply to any use of the In-App Purchase API in Your Application:

1. Use of the In-App Purchase API

1.1 You may use the In-App Purchase API only to enable end-users to access or receive content, functionality, or services that You make available for use within Your Application (e.g., digital books, additional game levels, access to a turn-by-turn map service). You may not use the In-App Purchase API to offer goods or services to be used outside of Your Application.

1.2 You must submit to Apple for review and approval all content, functionality, or services that You plan to provide through the use of the In-App Purchase API in accordance with these terms and the processes set forth in **Section 6 (Application Submission and Selection)** of the Agreement. For all submissions, You must provide the name, text description, price, unique identifier number, and other information that Apple reasonably requests (collectively, the "**Submission Description**"). Apple reserves the right to review the actual content, functionality or service that has been described in the Submission Descriptions at any time, including, but not limited to, in the submission process and after approval of the Submission Description by Apple. If You would like to provide additional content, functionality or services through the In-App Purchase API that are not described in Your Submission Description, then You must first submit a new or updated Submission Description for review and approval by Apple prior to making such items available through the use of the In-App Purchase API. Apple reserves the right to withdraw its approval of content, functionality, or services previously approved, and You agree to stop making any such content, functionality, or services available for use within Your Application.

1.3 All content, functionality, and services offered through the In-App Purchase API are subject to the Program Requirements for Applications, and after such content, services or functionality are added to a Licensed Application, they will be deemed part of the Licensed Application and will be subject to all the same obligations and requirements. For clarity, Applications that provide keyboard extension functionality may not use the In-App Purchase API within the keyboard extension itself; however, they may continue to use the In-App Purchase API in separate areas of the Application.

2. Additional Restrictions

2.1 You may not use the In-App Purchase API to enable an end-user to set up a pre-paid account to be used for subsequent purchases of content, functionality, or services, or otherwise create balances or credits that end-users can redeem or use to make purchases at a later time.

2.2 You may not enable end-users to purchase Currency of any kind through the In-App Purchase API, including but not limited to any Currency for exchange, gifting, redemption, transfer, trading or use in purchasing or obtaining anything within or outside of Your Application. "Currency" means any form of currency, points, credits, resources, content or other items or units recognized by a group of individuals or entities as representing a particular value and that can be transferred or circulated as a medium of exchange.

2.3 Content and services may be offered through the In-App Purchase API on a subscription basis (e.g., subscriptions to newspapers and magazines). Rentals of content, services or functionality through the In-App Purchase API are not allowed (e.g., use of particular content may not be restricted to a pre-determined, limited period of time).

2.4 You may not use the In-App Purchase API to send any software updates to Your Application or otherwise add any additional executable code to Your Application. An In-App Purchase item must either already exist in Your Application waiting to be unlocked, be streamed to Your Application after the In-App Purchase API transaction has been completed, or be downloaded to Your Application solely as data after such transaction has been completed.

2.5 You may not use the In-App Purchase API to deliver any items that contain content or materials of any kind (text, graphics, images, photographs, sounds, etc.) that in Apple's reasonable judgment may be found objectionable or inappropriate, for example, materials that may be considered obscene, pornographic, or defamatory.

2.6 With the exception of items of content that an end-user consumes or uses up within Your Application (e.g., virtual supplies such as construction materials) (a "Consumable"), any other content, functionality, services or subscriptions delivered through the use of the In-App Purchase API (e.g., a sword for a game) (a "Non-Consumable") must be made available to end-users in accordance with the same usage rules as Licensed Applications (e.g., any such content, services or functionality must be available to all of the devices associated with an end-user's account). You will be responsible for identifying Consumable items to Apple and for disclosing to end-users that Consumables will not be available for use on other devices.

3. Your Responsibilities

3.1 For each successfully completed transaction made using the In-App Purchase API, Apple will provide You with a transaction receipt. It is Your responsibility to verify the validity of such receipt prior to the delivery of any content, functionality, or services to an end-user and Apple will not be liable for Your failure to verify that any such transaction receipt came from Apple.

3.2 Unless Apple provides You with user interface elements, You are responsible for developing the user interface Your Application will display to end-users for orders made through the In-App Purchase API. You agree not to misrepresent, falsely claim, mislead or engage in any unfair or deceptive acts or practices regarding the promotion and sale of items through Your use of the In-App Purchase API, including, but not limited to, in the Licensed Application Information and any metadata that You submit through App Store Connect. You agree to comply with all applicable laws and regulations, including those in any jurisdictions in which You make content, functionality, services or subscriptions available through the use of the In-App Purchase API, including but not limited to consumer laws and export regulations.

3.3 Apple may provide hosting services for Non-Consumables that You would like to provide to Your end-users through the use of the In-App Purchase API. Even if Apple hosts such Non-Consumables on Your behalf, You are responsible for providing items ordered through the In-App Purchase API in a timely manner (i.e., promptly after Apple issues the transaction receipt, except in cases where You have disclosed to Your end-user that the item will be made available at a later time) and for complying with all applicable laws in connection therewith, including but not limited to, laws, rules and regulations related to cancellation or delivery of ordered items. You are responsible for maintaining Your own records for all such transactions.

3.4 You will not issue any refunds to end-users of Your Application, and You agree that Apple may issue refunds to end-users in accordance with the terms of Schedule 2.

4. Apple Services

4.1 From time to time, Apple may choose to offer additional services and functionality relating to In-App Purchase API transactions. Apple makes no guarantees that the In-App Purchase API or any Services will continue to be made available to You or that they will meet Your requirements, be uninterrupted, timely, secure or free from error, that any information that You

obtain from the In-App Purchase API or any Services will be accurate or reliable or that any defects will be corrected.

4.2 You understand that You will not be permitted to access or use the In-App Purchase API after expiration or termination of Your Agreement.

5. Your Acknowledgements. You acknowledge and agree that:
Apple may at any time, and from time to time, with or without prior notice to You (a) modify the In-App Purchase API, including changing or removing any feature or functionality, or (b) modify, deprecate, reissue or republish the In-App Purchase API. You understand that any such modifications may require You to change or update Your Applications at Your own cost in order to continue to use the In-App Purchase API. Apple has no express or implied obligation to provide, or continue to provide, the In-App Purchase API or any services related thereto and may suspend or discontinue all or any portion of thereof at any time. Apple shall not be liable for any losses, damages or costs of any kind incurred by You or any other party arising out of or related to any suspension, discontinuation or modification of the In-App Purchase API or any services related thereto. Apple makes no guarantees to You in relation to the availability or uptime of the In-App Purchase API or any other services that Apple may provide to You in connection therewith, and Apple is not obligated to provide any maintenance, technical or other support related thereto. Apple provides the In-App Purchase API to You for Your use with Your Application, and may provide services to You in connection therewith (e.g., hosting services for Non-Consumable items). Apple is not responsible for providing or unlocking any content, functionality, services or subscriptions that an end-user orders through Your use of the In-App Purchase API. You acknowledge and agree that any such items are made available by You, not Apple, to the end-user of Your Application, and You are solely liable and responsible for such items ordered through the use of the In-App Purchase API and for any such use of the In-App Purchase API in Your Application or for any use of services in connection therewith.

6. Use of Digital Certificates for In-App Purchase. When an end-user completes a transaction using the In-App Purchase API in Your Application, Apple will provide You with a transaction receipt signed with an Apple Certificate. It is Your responsibility to verify that such certificate and receipt were issued by Apple, as set forth in the Documentation. You are solely responsible for Your decision to rely on any such certificates and receipts. YOUR USE OF OR RELIANCE ON SUCH CERTIFICATES AND RECEIPTS IN CONNECTION WITH THE IN-APP PURCHASE API IS AT YOUR SOLE RISK. APPLE MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, AS TO MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, ACCURACY, RELIABILITY, SECURITY, OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS WITH RESPECT TO SUCH APPLE CERTIFICATES AND RECEIPTS. You agree that You will only use such receipts and certificates in accordance with the Documentation, and that You will not interfere or tamper with the normal operation of such digital certificates or receipts, including but not limited to any falsification or other misuse.

7. Additional Liability Disclaimer. APPLE SHALL NOT BE LIABLE FOR ANY DAMAGES OR LOSSES ARISING FROM THE USE OF THE IN-APP PURCHASE API AND ANY SERVICES, INCLUDING, BUT NOT LIMITED TO, (I) ANY LOSS OF PROFIT (WHETHER INCURRED DIRECTLY OR INDIRECTLY), ANY LOSS OF GOODWILL OR BUSINESS REPUTATION, ANY LOSS OF DATA SUFFERED, OR OTHER INTANGIBLE LOSS, (II) ANY CHANGES WHICH APPLE MAY MAKE TO THE IN-APP PURCHASE API OR ANY SERVICES, OR FOR ANY PERMANENT OR TEMPORARY CESSATION IN THE PROVISION OF THE IN-APP PURCHASE API OR ANY SERVICES (OR ANY FEATURES WITHIN THE SERVICES) PROVIDED THEREWITH, OR (III) THE DELETION OF, CORRUPTION OF, OR FAILURE TO PROVIDE ANY DATA TRANSMITTED BY OR THROUGH YOUR USE OF THE IN-APP PURCHASE API OR SERVICES. It is Your responsibility to maintain appropriate alternate backup of all Your information and data, including but not limited to any Non-Consumables that You may provide to Apple for hosting services.

Attachment 3
(to the Agreement)
Additional Terms for the Game Center

The following terms are in addition to the terms of the Agreement and apply to any use of the Game Center service by You or Your Application.

1. Use of the Game Center service

1.1 You and Your Application may not connect to or use the Game Center service in any way not expressly authorized by Apple. You agree to only use the Game Center service in accordance with this Agreement (including this Attachment 3), the Game Center Documentation and in accordance with all applicable laws. You understand that neither You nor Your Application will be permitted to access or use the Game Center service after expiration or termination of Your Agreement.

1.2 Apple may provide You with a unique identifier which is associated with an end-user's alias as part of the Game Center service (the "Player ID"). You agree to not display the Player ID to the end-user or to any third party, and You agree to only use the Player ID for differentiation of end-users in connection with Your use of the Game Center. You agree not to reverse look-up, trace, relate, associate, mine, harvest, or otherwise exploit the Player ID, aliases or other data or information provided by the Game Center service, except to the extent expressly permitted herein. For example, You will not attempt to determine the real identity of an end-user.

1.3 You will only use information provided by the Game Center service as necessary for providing services and functionality for Your Applications. For example, You will not host or export any such information to a third party service. Further, You agree not to transfer or copy any user information or data (whether individually or in the aggregate) obtained through the Game Center service to a third party except as necessary for providing services and functionality for Your Applications, and then only with express user consent and only if not otherwise prohibited in this Agreement.

1.4 You will not attempt to gain (or enable others to gain) unauthorized use or access to the Game Center service (or any part thereof) in any way, including but not limited to obtaining information from the Game Center service using any method not expressly permitted by Apple. For example, You may not use packet sniffers to intercept any communications protocols from systems or networks connected to the Game Center, scrape any data or user information from the Game Center, or use any third party software to collect information through the Game Center about players, game data, accounts, or service usage patterns.

2. Additional Restrictions

2.1 You agree not to harm or interfere with Apple's networks or servers, or any third party servers or networks connected to the Game Center service, or otherwise disrupt other developers' or end-users' use of the Game Center. You agree that, except for testing and development purposes, You will not create false accounts through the use of the Game Center service or otherwise use the Game Center service to misrepresent information about You or Your Application in a way that would interfere with an end-users' use of the Game Center service, e.g., creating inflated high scores through the use of cheat codes or falsifying the number of user accounts for Your Application.

2.2 You will not institute, assist, or enable any disruptions of the Game Center, such as through a denial of service attack, through the use of an automated process or service such as a spider, script, or bot, or through exploiting any bug in the Game Center service or Apple Software. You agree not to probe, test or scan for vulnerabilities in the Game Center service. You further

agree not to disable, spoof, hack, undermine or otherwise interfere with any data protection, security, verification or authentication mechanisms that are incorporated in or used by the Game Center service, or enable others to do so.

2.3 You will not transmit, store or otherwise make available any material that contains viruses or any other computer code, files or programs that may harm, disrupt or limit the normal operation of the Game Center or an iOS Product.

2.4 You agree not to use any portion of the Game Center service for sending any unsolicited, improper or inappropriate messages to end-users or for the purpose of poaching, phishing or spamming of Game Center users. You will not reroute (or attempt to reroute) users of the Game Center to another service using any information You obtain through the use of the Game Center service.

2.5 You shall not charge any fees to end-users for access to the Game Center service or for any data or information provided therein.

2.6 To the extent that Apple permits You to manage certain Game Center features and functionality for Your Application through App Store Connect (e.g., the ability to block fraudulent users or eliminate suspicious leaderboard scores from Your Application's leaderboard), You agree to use such methods only when You have a reasonable belief that such users or scores are the result of misleading, fraudulent, improper, unlawful or dishonest acts.

3. Your Acknowledgements. You acknowledge and agree that:

3.1 Apple may at any time, and from time to time, with or without prior notice to You (a) modify the Game Center service, including changing or removing any feature or functionality, or (b) modify, deprecate, reissue or republish the Game Center APIs or related APIs. You understand that any such modifications may require You to change or update Your Applications at Your own cost. Apple has no express or implied obligation to provide, or continue to provide, the Game Center service and may suspend or discontinue all or any portion of the Game Center service at any time. Apple shall not be liable for any losses, damages or costs of any kind incurred by You or any other party arising out of or related to any such service suspension or discontinuation or any such modification of the Game Center service or Game Center APIs.

3.2 Apple makes no guarantees to You in relation to the availability or uptime of the Game Center service and is not obligated to provide any maintenance, technical or other support for such service. Apple reserves the right to remove Your access to the Game Center service at any time in its sole discretion. Apple may monitor and collect information (including but not limited to technical and diagnostic information) about Your usage of the Game Center service to aid Apple in improving the Game Center and other Apple products or services and to verify Your compliance with this Agreement.

4. Additional Liability Disclaimer. APPLE SHALL NOT BE LIABLE FOR ANY DAMAGES OR LOSSES ARISING FROM ANY INTERRUPTIONS TO THE GAME CENTER OR ANY SYSTEM FAILURES, NETWORK ATTACKS, SCHEDULED OR UNSCHEDULED MAINTENANCE, OR OTHER INTERRUPTIONS.

Attachment 4
(to the Agreement)
Additional Terms for the use of iCloud

The following terms are in addition to the terms of the Agreement and apply to Your use of the iCloud service for software development and testing in connection with Your Application, or Web Software.

1. Use of iCloud

1.1 Your Applications and/or Web Software may access the iCloud service only if You have been assigned an entitlement by Apple. You agree not to access the iCloud service, or any content, data or information contained therein, other than through the iCloud Storage APIs, CloudKit APIs or via the CloudKit dashboard provided as part of the Program. You agree not to share Your entitlement with any third party or use it for any purposes not expressly permitted by Apple. You agree to use the iCloud service, the iCloud Storage APIs, and the CloudKit APIs only as expressly permitted by this Agreement and the iCloud Documentation, and in accordance with all applicable laws and regulations. Further, Your Web Software is permitted to access and use the iCloud service (e.g., to store the same type of data that is retrieved or updated in a Licensed Application) only so long as Your use of the iCloud service in such Web Software is comparable to Your use in the corresponding Licensed Application, as determined in Apple's sole discretion. In the event Apple Services permit You to use more than Your allotment of storage containers in iCloud in order to transfer data to another container for any reason, You agree to only use such additional container(s) for a reasonable limited time to perform such functions and not to increase storage and transactional allotments.

1.2 You understand that You will not be permitted to access or use the iCloud service for software development or testing after expiration or termination of Your Agreement; however end-users who have Your Applications or Web Software installed and who have a valid end-user account with Apple to use iCloud may continue to access their user-generated documents, private containers and files that You have chosen to store in such end-user's account via the iCloud Storage APIs or the CloudKit APIs in accordance with the applicable iCloud terms and conditions and these terms. You agree not to interfere with an end-user's ability to access iCloud (or the end-user's own user-generated documents, private containers and files) or to otherwise disrupt their use of iCloud in any way and at any time. With respect to data You store in public containers through the CloudKit APIs (whether generated by You or the end-user), Apple reserves the right to suspend access to or delete such data, in whole or in part, upon expiration or termination of Your Agreement, or as otherwise specified by Apple in the CloudKit dashboard.

1.3 Your Application is permitted to use the iCloud Storage APIs only for the purpose of storage and retrieval of key value data (e.g., a list of stocks in a finance App, settings for an App) for Your Applications and Web Software and for purposes of enabling Your end-users to access user-generated documents and files through the iCloud service. Your Application or Web Software application is permitted to use the CloudKit APIs for storing, retrieving, and querying of structured data that You choose to store in public or private containers in accordance with the iCloud Documentation. You agree not to knowingly store any content or materials via the iCloud Storage APIs or CloudKit APIs that would cause Your Application to violate any of the iCloud terms and conditions or the Program Requirements for Your Applications (e.g., Your Application may not store illegal or infringing materials).

1.4 You may allow a user to access their user-generated documents and files from iCloud through the use of Your Applications as well as from Web Software. However, You may not share key value data from Your Application with other Applications or Web Software, unless You are sharing such data among different versions of the same title, or You have user consent.

1.5 You are responsible for any content and materials that You store in iCloud through the use of the CloudKit APIs and iCloud Storage APIs and must take reasonable and appropriate steps to protect information You store through the iCloud service. With respect to third party claims related to content and materials stored by Your end-users in Your Applications through the use of the iCloud Storage APIs or CloudKit APIs (e.g., user-generated documents, end-user posts in public containers), You agree to be responsible for properly handling and promptly processing any such claims, including but not limited to Your compliance with notices sent pursuant to the Digital Millennium Copyright Act (DMCA).

1.6 Unless otherwise expressly permitted by Apple in writing, You will not use iCloud, the iCloud Storage APIs, CloudKit APIs, or any component or function thereof, to create, receive, maintain or transmit any sensitive, individually-identifiable health information, including "protected health information" (as such term is defined at 45 C.F.R § 160.103), or use iCloud in any manner that would make Apple (or any Apple Subsidiary) Your or any third party's "business associate" as such term is defined at 45 C.F.R. § 160.103. You agree to be solely responsible for complying with any reporting requirements under law or contract arising from Your breach of this Section.

2. Additional Requirements

2.1 You understand there are storage capacity, transmission, and transactional limits for the iCloud service, both for You as a developer and for Your end-users. If You reach or Your end-user reaches such limits, then You or Your end-user may be unable to use the iCloud service until You or Your end-user have removed enough data from the service to meet the capacity limits, increased storage capacity or otherwise modified Your usage of iCloud, and You or Your end-user may be unable to access or retrieve data from iCloud during this time.

2.2 You may not charge any fees to users for access to or use of the iCloud service through Your Applications or Web Software, and You agree not to sell access to the iCloud service in any other way, including but not limited to reselling any part of the service. You will only use the iCloud service in Your Application or Web Software to provide storage for an end-user who has a valid end-user iCloud account with Apple and only for use in accordance with the terms of such user account, except that You may use the CloudKit APIs to store of data in public containers for access by end-users regardless of whether such users have iCloud accounts. You will not induce any end-user to violate the terms of their applicable iCloud service agreement with Apple or to violate any Apple usage policies for data or information stored in the iCloud service.

2.3 You may not excessively use the overall network capacity or bandwidth of the iCloud service or otherwise burden such service with unreasonable data loads or queries. You agree not to harm or interfere with Apple's networks or servers, or any third party servers or networks connected to the iCloud, or otherwise disrupt other developers' or users' use of the iCloud service.

2.4 You will not disable or interfere with any warnings, system settings, notices, or notifications that are presented to an end-user of the iCloud service by Apple.

3. Your Acknowledgements

You acknowledge and agree that:

3.1 Apple may at any time, with or without prior notice to You (a) modify the iCloud Storage APIs or the CloudKit APIs, including changing or removing any feature or functionality, or (b) modify, deprecate, reissue or republish such APIs. You understand that any such modifications may require You to change or update Your Applications or Web Software at Your own cost. Apple has no express or implied obligation to provide, or continue to provide, the iCloud service and may suspend or discontinue all or any portion of the iCloud service at any time. Apple shall

not be liable for any losses, damages or costs of any kind incurred by You or any other party arising out of or related to any such service suspension or discontinuation or any such modification of the iCloud service, iCloud Storage APIs or the CloudKit APIs.

3.2 The iCloud service is not available in all languages or in all countries and Apple makes no representation that the iCloud service is appropriate or available for use in any particular location. To the extent You choose to provide access to the iCloud service in Your Applications or Web Software through the iCloud Storage APIs or CloudKit APIs (e.g., to store data in a public or private container), You do so at Your own initiative and are responsible for compliance with any applicable laws or regulations.

3.3 Apple makes no guarantees to You in relation to the availability or uptime of the iCloud service and is not obligated to provide any maintenance, technical or other support for the iCloud service. Apple is not responsible for any expenditures, investments, or commitments made by You in connection with the iCloud service, or for any use of or access to the iCloud service.

3.4 Apple reserves the right to suspend or revoke Your access to the iCloud service or impose limits on Your use of the iCloud service at any time in Apple's sole discretion. In addition, Apple may impose or adjust the limit of transactions Your Applications or Web Software may send or receive through the iCloud service or the resources or capacity that they may use at any time in Apple's sole discretion.

3.5 Apple may monitor and collect information (including but not limited to technical and diagnostic information) about usage of the iCloud service through the iCloud Storage APIs, CloudKit APIs, or CloudKit dashboard, in order to aid Apple in improving the iCloud service and other Apple products or services; provided however that Apple will not access or disclose any end-user data stored in a private container through CloudKit, any Application data stored in a public container through CloudKit, or any user-generated documents, files or key value data stored using the iCloud Storage APIs and iCloud service, unless Apple has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to comply with a legal or regulatory process or request, or unless otherwise requested by an end-user with respect to data stored via the iCloud Storage APIs in that end-user's iCloud account or in that end-user's private container via the CloudKit APIs.

3.6 Further, to the extent that You store any personal information relating to an individual or any information from which an individual can be identified (collectively, "Personal Data") in the iCloud service through the use of the iCloud Storage APIs or CloudKit APIs, You agree that Apple (and any applicable Apple Subsidiary for purposes of this Section 3.6) will act as Your agent for the processing, storage and handling of any such Personal Data. Apple agrees to ensure that any persons authorized to process such Personal Data have agreed to maintain confidentiality (whether through terms or under an appropriate statutory obligation). Apple shall have no right, title or interest in such Personal Data solely as a result of Your use of the iCloud service. You agree that You are solely liable and responsible for ensuring Your compliance with all applicable laws, including privacy and data protection laws, regarding the use or collection of data and information through the iCloud service. You are also responsible for all activity related to such Personal Data, including but not limited to, monitoring such data and activity, preventing and addressing inappropriate data and activity, and removing and terminating access to data. Further, You are responsible for safeguarding and limiting access to such Personal Data by Your personnel and for the actions of Your personnel who are permitted access to use the iCloud service on Your behalf. Personal Data provided by You and Your users to Apple through the iCloud service may be used by Apple only as necessary to provide and improve the iCloud service and to perform the following actions on Your behalf. Apple shall:

(a) use and handle such Personal Data only in accordance with the instructions and permissions from You set forth herein, as well as applicable laws, regulations, accords, or treaties. In the EEA

and Switzerland, Personal Data will be handled by Apple only in accordance with the instructions and permissions from You set forth herein unless otherwise required by European Union or Member State Law, in which case Apple will notify You of such other legal requirement (except in limited cases where Apple is prohibited by law from doing so);
(b) provide You with reasonable means to manage any user access, deletion, or restriction requests as defined in applicable law. In the event of an investigation of You arising from Your good faith use of the iCloud service by a data protection regulator or similar authority regarding such Personal Data, Apple shall provide You with reasonable assistance and support;
(c) notify You by any reasonable means Apple selects, without undue delay and taking account of applicable legal requirements applying to You which mandate notification within a specific timeframe, if Apple becomes aware that Your Personal Data has been altered, deleted or lost as a result of any unauthorized access to the Service. You are responsible for providing Apple with Your updated contact information for such notification purposes in accordance with the terms of this Agreement;
(d) make available to You the information necessary to demonstrate compliance obligations set forth in Article 28 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (GDPR) and to allow for and contribute to audits required under these provisions; provided however that You agree that Apple's ISO 27001 and 27018 certifications shall be considered sufficient for such required audit purposes;
(e) assist You, by any reasonable means Apple selects, in ensuring compliance with its obligations pursuant to Articles 33 to 36 of the GDPR. If Apple receives a third party request for information You have stored in the iCloud service, then unless otherwise required by law or the terms of such request, Apple will notify You of its receipt of the request and notify the requester of the requirement to address such request to You. Unless otherwise required by law or the request, You will be responsible for responding to the request;
(f) use industry-standard measures to safeguard Personal Data during the transfer, processing and storage of Personal Data. Encrypted Personal Data may be stored at Apple's geographic discretion; and
(g) ensure that where Personal Data, arising in the context of this Agreement, is transferred from the EEA or Switzerland it is only to a third country that ensures an adequate level of protection or using the Model Contract Clauses/Swiss Transborder Data Flow Agreement which will be provided to You upon request if you believe that Personal Data is being transferred.

4. Additional Liability Disclaimer. NEITHER APPLE NOR ITS SERVICE PROVIDERS SHALL BE LIABLE FOR ANY DAMAGES OR LOSSES ARISING FROM ANY USE, MISUSE, RELIANCE ON, INABILITY TO USE, INTERRUPTION, SUSPENSION OR TERMINATION OF iCLOUD, iCLOUD STORAGE APIS, OR CLOUDKIT APIS, OR FOR ANY UNAUTHORIZED ACCESS TO, ALTERATION OF, OR DELETION, DESTRUCTION, DAMAGE, LOSS OR FAILURE TO STORE ANY OF YOUR DATA OR ANY END-USER DATA OR ANY CLAIMS ARISING FROM ANY USE OF THE FOREGOING BY YOUR END-USERS, INCLUDING ANY CLAIMS REGARDING DATA PROCESSING OR INAPPROPRIATE OR UNAUTHORIZED DATA STORAGE OR HANDLING BY YOU IN VIOLATION OF THIS AGREEMENT.

Attachment 5
(to the Agreement)
Additional Terms for Passes

The following terms are in addition to the terms of the Agreement and apply to Your development and distribution of Passes:

1. Pass Type ID Usage and Restrictions

You may use the Pass Type ID only for purposes of digitally signing Your Pass for use with Wallet and/or for purposes of using the APN service with Your Pass. You may distribute Your Pass Type ID as incorporated into Your Pass in accordance with **Section 2** below only so long as such distribution is under Your own trademark or brand. To the extent that You reference a third party's trademark or brand within Your Pass (e.g., a store coupon for a particular good), You represent and warrant that You have any necessary rights. You agree not to share, provide or transfer Your Pass Type ID to any third party (except for a Service Provider and only to the limited extent permitted herein), nor use Your Pass Type ID to sign a third party's pass.

2. Pass Distribution; Marketing Permissions

2.1 Subject to the terms of this Agreement, You may distribute Your Passes to end-users by the web, email, or an Application. You understand that Passes must be accepted by such users before they will be loaded into Wallet and that Passes can be removed or transferred by such users at any time.

2.2 By distributing Your Passes in this manner, You represent and warrant to Apple that Your Passes comply with the Documentation and Program Requirements then in effect and the terms of this Attachment 5. Apple shall not be responsible for any costs, expenses, damages, losses (including without limitation lost business opportunities or lost profits) or other liabilities You may incur as a result of distributing Your Passes in this manner.

2.3 You agree to state on the Pass Your name and address, and the contact information (telephone number; email address) to which any end-user questions, complaints, or claims with respect to Your Pass should be directed. You will be responsible for attaching or otherwise including, at Your discretion, any relevant end-user usage terms with Your Pass. Apple will not be responsible for any violations of Your end-user usage terms. You will be solely responsible for all user assistance, warranty and support of Your Pass. You may not charge any fees to end-users in order to use Wallet to access Your Pass.

2.4 By distributing Your Passes as permitted in this Agreement, You hereby permit Apple to use (i) screen shots of Your Pass; (ii) trademarks and logos associated with Your Pass; and (iii) Pass Information, for promotional purposes in marketing materials and gift cards, excluding those portions which You do not have the right to use for promotional purposes and which You identify in writing to Apple. You also permit Apple to use images and other materials that You may provide to Apple, at Apple's reasonable request, for promotional purposes in marketing materials and gift cards.

3. Additional Pass Requirements

3.1 Apple may provide You with templates to use in creating Your Passes, and You agree to choose the relevant template for Your applicable use (e.g., You will not use the boarding pass template for a movie ticket).

3.2 Passes may only operate and be displayed in Wallet, which is Apple's designated container area for the Pass, through Wallet on the lock screen of a compatible Apple-branded product in accordance with the Documentation.

3.3. Notwithstanding anything else in **Section 3.3.9** of the Agreement, with prior user consent, You and Your Pass may share user and/or device data with Your Application so long as such sharing is for the purpose of providing a service or function that is directly relevant to the use of the Pass and/or Application, or to serve advertising in accordance with **Sections 3.3.12** of the Agreement.

3.4 If You would like to use embedded Near Field Communication (NFC) technology with Your Pass, then You may request an Apple Certificate for the use of NFC with a Pass from the Developer web portal. Apple will review Your request and may provide You with a separate agreement for the use of such Apple Certificate. Apple reserves the right to not provide You with such Apple Certificate.

4. Apple's Right to Review Your Pass; Revocation. You understand and agree that Apple reserves the right to review and approve or reject any Pass that You would like to distribute for use by Your end-users, or that is already in use by Your end-users, at any time during the Term of this Agreement. If requested by Apple, You agree to promptly provide such Pass to Apple. You agree not to attempt to hide, misrepresent, mislead, or obscure any features, content, services or functionality in Your Pass from Apple's review or otherwise hinder Apple from being able to fully review such Pass, and, You agree to cooperate with Apple and answer questions and provide information and materials reasonably requested by Apple regarding such Pass. If You make any changes to Your Pass after submission to Apple, You agree to notify Apple and, if requested by Apple, resubmit Your Pass prior to any distribution of the modified Pass to Your end-users. Apple reserves the right to revoke Your Pass Type ID and reject Your Pass for distribution to Your end-users for any reason and at any time in its sole discretion, even if Your Pass meets the Documentation and Program Requirements and terms of this Attachment 5; and, in that event, You agree that You may not distribute such Pass to Your end-users.

5. Additional Liability Disclaimer. APPLE SHALL NOT BE LIABLE FOR ANY DAMAGES OR LOSSES ARISING FROM ANY USE, DISTRIBUTION, MISUSE, RELIANCE ON, INABILITY TO USE, INTERRUPTION, SUSPENSION, OR TERMINATION OF WALLET, YOUR PASS TYPE ID, YOUR PASSES, OR ANY SERVICES PROVIDED IN CONNECTION THEREWITH, INCLUDING BUT NOT LIMITED TO ANY LOSS OR FAILURE TO DISPLAY YOUR PASS IN WALLET OR ANY END-USER CLAIMS ARISING FROM ANY USE OF THE FOREGOING BY YOUR END-USERS.

Attachment 6
(to the Agreement)
Additional Terms for the use of the Apple Maps Service

The following terms are in addition to the terms of the Agreement and apply to any use of the Apple Maps Service in Your Application, website, or web application.

1. Use of the Maps Service

1.1 Your Application may access the Apple Maps Service only via the MapKit API or through MapKit JS, and Your website or web application may access the Apple Maps Service only via MapKit JS. You agree not to access the Apple Maps Service or the Map Data other than through the MapKit API or MapKit JS, as applicable, and You agree that Your use of the Apple Maps Service in Your Applications, websites, or web applications must comply with the Program Requirements.

1.2 You will use the Apple Maps Service and Map Data only as necessary for providing services and functionality for Your Application, website, or web application. You agree to use the Apple Maps Service, MapKit API and MapKit JS only as expressly permitted by this Agreement (including but not limited to this Attachment 6) and the MapKit and MapKit JS Documentation, and in accordance with all applicable laws and regulations. MapKit JS may not be used in Your website and/or application running on non-Apple hardware for the following commercial purposes: fleet management (including dispatch), asset tracking, enterprise route optimization, or where the primary purpose of such website and/or application is to assess vehicle insurance risk.

1.3 You acknowledge and agree that results You receive from the Apple Maps Service may vary from actual conditions due to variable factors that can affect the accuracy of the Map Data, such as weather, road and traffic conditions, and geopolitical events.

2. Additional Restrictions

2.1 Neither You nor Your Application, website or web application may remove, obscure or alter Apple's or its licensors' copyright notices, trademarks, logos, or any other proprietary rights or legal notices, documents or hyperlinks that may appear in or be provided through the Apple Maps Service.

2.2 You will not use the Apple Maps Service in any manner that enables or permits bulk downloads or feeds of the Map Data, or any portion thereof, or that in any way attempts to extract, scrape or reutilize any portions of the Map Data. For example, neither You nor Your Application may use or make available the Map Data, or any portion thereof, as part of any secondary or derived database.

2.3 Except to the extent expressly permitted herein, You agree not to copy, modify, translate, create a derivative work of, publish or publicly display the Map Data in any way. Further, You may not use or compare the data provided by the Apple Maps Service for the purpose of improving or creating another mapping service. You agree not to create or attempt to create a substitute or similar service through use of or access to the Apple Maps Service.

2.4 Your Application, website, or web application may display the Map Data only as permitted herein, and when displaying it on a map, You agree that it will be displayed only on an Apple map provided through the Apple Maps Service. Further, You may not surface Map Data within Your Application, website, or web application without displaying the corresponding Apple map (e.g., if You surface an address result through the Apple Maps Service, You must display the corresponding map with the address result).

2.5 Unless otherwise expressly permitted in the MapKit Documentation or MapKit JS

Documentation, Map Data may not be cached, pre-fetched, or stored by You or Your Application, website, or web application other than on a temporary and limited basis solely to improve the performance of the Apple Maps Service with Your Application, website, or web application.

2.6 You may not charge any fees to end-users solely for access to or use of the Apple Maps Service through Your Application, website, or web application, and You agree not to sell access to the Apple Maps Service in any other way.

2.7 You acknowledge and agree that Apple may impose restrictions on Your usage of the Apple Maps Service (e.g., limiting the number of transactions Your Application can make through the MapKit API) or may revoke or remove Your access to the Apple Maps Service (or any part thereof) at any time in its sole discretion. Further, You acknowledge and agree that results You may receive from the Apple Maps Service may vary from actual conditions due to variable factors that can affect the accuracy of Map Data, such as road or weather conditions.

3. Your Acknowledgements. You acknowledge and agree that:

3.1 Apple may at any time, with or without prior notice to You (a) modify the Apple Maps Service and/or the MapKit API or MapKit JS, including changing or removing any feature or functionality, or (b) modify, deprecate, reissue or republish the MapKit API or MapKit JS. You understand that any such modifications may require You to change or update Your Applications, website, or web applications at Your own cost. Apple has no express or implied obligation to provide, or continue to provide, the Apple Maps Service and may suspend or discontinue all or any portion of the Apple Maps Service at any time. Apple shall not be liable for any losses, damages or costs of any kind incurred by You or any other party arising out of or related to any such service suspension or discontinuation or any such modification of the Apple Maps Service, MapKit API, or MapKit JS.

3.2 The Apple Maps Service may not be available in all countries or languages, and Apple makes no representation that the Apple Maps Service is appropriate or available for use in any particular location. To the extent You choose to provide access to the Apple Maps Service in Your Applications, website, or web applications or through the MapKit API or MapKit JS, You do so at Your own initiative and are responsible for compliance with any applicable laws.

4. Apple's Right to Review Your MapKit JS Implementation. You understand and agree that Apple reserves the right to review and approve or reject Your implementation of MapKit JS in Your Application, website, or web applications, at any time during the Term of this Agreement. If requested by Apple, You agree to promptly provide information regarding Your implementation of MapKit JS to Apple. You agree to cooperate with Apple and answer questions and provide information and materials reasonably requested by Apple regarding such implementation. Apple reserves the right to revoke Your MapKit JS keys and similar credentials at any time in its sole discretion, even if Your use of MapKit JS meets the Documentation and Program Requirements and terms of this Attachment. By way of example only, Apple may do so if Your MapKit JS implementation places an excessive and undue burden on the Apple Maps Service, obscures or removes the Apple Maps logo or embedded links when displaying a map, or uses the Apple Maps Service with corresponding offensive or illegal map content.

5. Additional Liability Disclaimer. NEITHER APPLE NOR ITS LICENSORS OR SERVICE PROVIDERS SHALL BE LIABLE FOR ANY DAMAGES OR LOSSES ARISING FROM ANY USE, MISUSE, RELIANCE ON, INABILITY TO USE, INTERRUPTION, SUSPENSION OR TERMINATION OF THE APPLE MAPS SERVICE, INCLUDING ANY INTERRUPTIONS DUE TO SYSTEM FAILURES, NETWORK ATTACKS, OR SCHEDULED OR UNSCHEDULED MAINTENANCE.

Attachment 7
(to the Agreement)
Additional Terms for Safari Extensions

The following terms are in addition to the terms of the Agreement and apply to Safari Extensions signed with an Apple Certificate:

1.1 Safari Extension Requirements
If You would like to distribute Your Safari Extension signed with an Apple Certificate, then You agree to abide by the following requirements for such Safari Extensions, as they may be modified by Apple from time to time:

- Your Safari Extension must not contain any malware, malicious or harmful code, or other internal component (e.g. computer viruses, trojan horses, “backdoors”), which could damage, destroy, or adversely affect Apple hardware, software or services, or other third party software, firmware, hardware, data, systems, services, or networks;

- Your Safari Extensions must not be designed or marketed for the purpose of harassing, abusing, stalking, spamming, misleading, defrauding, threatening or otherwise violating the legal rights (such as the rights of privacy and publicity) of others. Further, You may not create a Safari Extension that tracks the behavior of a user (e.g., their browsing sites) without their express consent;

- Your Safari Extension must only operate in the designated container area for the Safari Extension, and must not disable, override or otherwise interfere with any Apple-implemented system alerts, warnings, display panels, consent panels and the like;

- Your Safari Extension must have a single purpose and updates must not change the single purpose of Your Safari Extension. You agree to accurately represent the features and functionality of Your Safari Extension to the user and to act in accordance with such representations. For example, You must not redirect user searches to a different search provider than the one previously selected by the user in Safari without their express consent. In addition, Your Safari Extension may not redirect a link (or any affiliate link) on a website unless that behavior is disclosed to the user. You agree not to conceal the features or functionality of Your Safari Extension (e.g., containing obfuscated code);

- Your Safari Extension must not be bundled with an app that has a different purpose than the Safari Extension. Your Safari Extension must not inject ads into a website and may not display pop up ads. You must not script or automate turning on Your Safari Extension or enable others to do so; and

- Safari Extensions must not interfere with security, user interface, user experience, features or functionality of Safari, macOS, iOS, or other Apple-branded products.

1.2 Compliance; Certificates. Your Safari Extensions must comply with the Documentation and all applicable laws and regulations, including those in any jurisdictions in which such Safari Extensions may be offered or made available. You understand that Apple may revoke the Apple Certificates used to sign Your Safari Extensions at any time, in its sole discretion. Further, You acknowledge and agree that Apple may block Your Safari Extension (such that it may be unavailable or inaccessible to Safari users) if it does not comply with the requirements set forth above in this **Section 1.1** or otherwise adversely affects users of Safari or Apple-branded products.

Schedule 1

1. Appointment of Agent

1.1 You hereby appoint Apple and Apple Subsidiaries (collectively "Apple") as: (i) Your agent for the marketing and delivery of the Licensed Applications to end-users located in those countries listed on Exhibit A, Section 1 to this Schedule 1, subject to change; and (ii) Your commissionaire for the marketing and delivery of the Licensed Applications to end-users located in those countries listed on Exhibit A, Section 2 to this Schedule 1, subject to change, during the Delivery Period. The most current list of App Store countries among which You may select shall be set forth in the App Store Connect tool and the Custom App Distribution Site and may be updated by Apple from time to time. You hereby acknowledge that Apple will market and make the Licensed Applications available for download by end-users, through one or more App Stores or the Custom App Distribution Site, for You and on Your behalf. For purposes of this Schedule 1, the following terms apply:

"Custom App" or "Custom Application" means a Licensed Application custom developed by You for use by specific organizations or third-party business customers, including proprietary Licensed Applications developed for Your organization's internal use.

(a) "You" shall include App Store Connect users authorized by You to submit Licensed Applications and associated metadata on Your behalf; and

(b) "end-user" includes individual purchasers as well as eligible users associated with their account via Family Sharing. For institutional customers, "end-user" shall mean the individual authorized to use the Licensed Application, the institutional administrator responsible for management of installations on shared devices, as well as authorized institutional purchasers themselves, including educational institutions approved by Apple, which may acquire the Licensed Applications for use by their employees, agents, and affiliates.

(c) For the purposes of this Schedule 1, the term "Licensed Application" shall include any content, functionality, extensions, stickers, or services offered in the software application.

"Volume Content Service" means an Apple service that offers the ability to obtain Custom Applications and make purchases of Licensed Applications in bulk subject to the Volume Content Terms, conditions, and requirements.

1.2 In furtherance of Apple's appointment under Section 1.1 of this Schedule 1, You hereby authorize and instruct Apple to:

(a) market, solicit and obtain orders on Your behalf for Licensed Applications from end-users located in the countries identified by You in the App Store Connect tool;

(b) provide hosting services to You subject to the terms of the Agreement, in order to allow for the storage of, and end-user access to, the Licensed Applications and to enable third party hosting of such Licensed Applications solely as otherwise licensed or authorized by Apple;

(c) make copies of, format, and otherwise prepare Licensed Applications for acquisition and download by end-users, including adding the Security Solution and other optimizations identified in the Agreement;

(d) allow or, in the case of cross-border assignments of certain purchases, arrange for end-users to access and re-access copies of the Licensed Applications, so that end-users may acquire from You and electronically download those Licensed Applications, Licensed Application Information,

and associated metadata through one or more App Stores or the Custom App Distribution Site, and You hereby authorize distribution of Your Licensed Applications under this Schedule 1 to end-users with accounts associated with another end-user's via Family Sharing. You also hereby authorize distribution of Your Licensed Applications under this Schedule 1 for use by multiple end users under a single Apple ID when the Licensed Application is provided to such end-users through Apple Configurator in accordance with the Apple Configurator software license agreement or requested by a single institutional customer via Custom App Distribution for use by its end-users and/or for installation on devices with no associated iTunes Account that are owned or controlled by that institutional customer in accordance with the Volume Content Terms, conditions, and program requirements;

(e) use (i) screen shots, previews, and/or up to 30 second excerpts of the Licensed Applications; (ii) trademarks and logos associated with the Licensed Applications; and (iii) Licensed Application Information, for promotional purposes in marketing materials and gift cards and in connection with vehicle displays, excluding those portions of the Licensed Applications, trademarks or logos, or Licensed Application Information which You do not have the right to use for promotional purposes, and which You identify in writing at the time that the Licensed Applications are delivered by You to Apple under Section 2.1 of this Schedule 1, and use images and other materials that You may provide to Apple, at Apple's reasonable request, for promotional purposes in marketing materials and gift cards and in connection with vehicle displays. In addition, and subject to the limitation set forth above, You agree that Apple may use screen shots, icons, and up to 30 second excerpts of Your Licensed Applications for use at Apple Developer events (e.g., WWDC, Tech Talks) and in developer documentation;

(f) otherwise use Licensed Applications, Licensed Application Information and associated metadata as may be reasonably necessary in the marketing and delivery of the Licensed Applications in accordance with this Schedule 1. You agree that no royalty or other compensation is payable for the rights described above in Section 1.2 of this Schedule 1; and

(g) facilitate distribution of pre-release versions of Your Licensed Applications ("Beta Testing") to end-users designated by You in accordance with the Agreement, availability, and other program requirements as updated from time to time in the App Store Connect tool. For the purposes of such Beta Testing, You hereby waive any right to collect any purchase price, proceeds or other remuneration for the distribution and download of such pre-release versions of Your Licensed Application. You further agree that You shall remain responsible for the payment of any royalties or other payments to third parties relating to the distribution and user of Your pre-release Licensed Applications, as well as compliance with any and all laws for territories in which such Beta Testing takes place. For the sake of clarity, no commission shall be owed to Apple with respect to such distribution.

1.3 The parties acknowledge and agree that their relationship under this Schedule 1 is, and shall be, that of principal and agent, or principal and commissionaire, as the case may be, as described in Exhibit A, Section 1 and Exhibit A, Section 2 respectively, and that You, as principal, are, and shall be, solely responsible for any and all claims and liabilities involving or relating to, the Licensed Applications, as provided in this Schedule 1. The parties acknowledge and agree that Your appointment of Apple as Your agent or commissionaire, as the case may be, under this Schedule 1 is non-exclusive. You hereby represent and warrant that You own or control the necessary rights in order to appoint Apple and Apple Subsidiaries as Your worldwide agent and/or commissionaire for the delivery of Your Licensed Applications, and that the fulfillment of such appointment by Apple and Apple Subsidiaries shall not violate or infringe the rights of any third party.

1.4 For purposes of this Schedule 1, the "Delivery Period" shall mean the period beginning on the Effective Date of the Agreement, and expiring on the last day of the Agreement or any renewal thereof; provided, however, that Apple's appointment as Your agent shall survive expiration of the Agreement for a reasonable phase-out period not to exceed thirty (30) days and

further provided that, solely with respect to Your end-users, subsections 1.2(b), (c), and (d) of this Schedule 1 shall survive termination or expiration of the Agreement unless You indicate otherwise pursuant to sections 4.1 and 6.2 of this Schedule 1.

1.5 All of the Licensed Applications delivered by You to Apple under Section 2.1 of this Schedule 1 shall be made available by Apple for download by end-users at no charge. Apple shall have no duty to collect any fees for the Licensed Applications for any end-user and shall have no payment obligation to You with respect to any of those Licensed Applications under this Schedule 1. In the event that You intend to charge end-users a fee for any Licensed Application or In-App Purchase, You must enter (or have previously entered) into a separate extension of this agreement (Schedule 2) with Apple with respect to that Licensed Application. In the event that You intend to charge end-users a fee for any Custom Apps, You must enter (or have previously entered) into a separate extension of this agreement (Schedule 3) with Apple with respect to that Custom App.

2. Delivery of the Licensed Applications to Apple

2.1 You will deliver to Apple, at Your sole expense, using the App Store Connect tool or other mechanism provided by Apple, the Licensed Applications, Licensed Application Information and associated metadata, in a format and manner prescribed by Apple, as required for the delivery of the Licensed Applications to end-users in accordance with this Schedule 1. Metadata You deliver to Apple under this Schedule 1 will include: (i) the title and version number of each of the Licensed Applications; (ii) the countries You designate, in which You wish Apple to allow end-users to download those Licensed Applications; (iii) the end-users You designate as authorized downloaders of the Custom App; (iv) any copyright or other intellectual property rights notices; (v) Your privacy policy; (vi) Your end-user license agreement ("EULA"), if any, in accordance with Section 3.2 of this Schedule 1; and (vii) any additional metadata set forth in the Documentation and/or the App Store Connect Tool as may be updated from time to time, including metadata designed to enhance search and discovery for content on Apple-branded hardware.

2.2 All Licensed Applications will be delivered by You to Apple using software tools, a secure FTP site address and/or such other delivery methods as prescribed by Apple.

2.3 You hereby certify that all of the Licensed Applications You deliver to Apple under this Schedule 1 are authorized for export from the United States to each of the countries designated by You under Section 2.1 hereof, in accordance with the requirements of all applicable laws, including but not limited to the United States Export Administration Regulations, 15 C.F.R. Parts 730-774 and the International Traffic in Arms Regulations 22 C.F.R. Parts 120-130. Without limiting the generality of this Section 2.3, You certify that (i) none of the Licensed Applications contains, uses or supports any data encryption or cryptographic functions; or (ii) in the event that any Licensed Application contains, uses or supports any such data encryption or cryptographic functionality, You certify that You have complied with the United States Export Administration Regulations, and are in possession of, and will, upon request, provide Apple with a PDF copy of Your Encryption Registration Number (ERN), or export classification ruling (CCATS) issued by the United States Commerce Department, Bureau of Industry and Security and PDF copies of appropriate authorizations from other countries that mandate import authorizations for that Licensed Application, as required. You acknowledge that Apple is relying upon Your certification in this Section 2.3 in allowing end-users to access and download the Licensed Applications under this Schedule 1. Except as provided in this Section 2.3, Apple will be responsible for compliance with the requirements of the Export Administration Regulations in allowing end-users to access and download the Licensed Applications under this Schedule 1.

2.4 You shall be responsible for determining and implementing any age ratings or parental advisory warnings required by the applicable government regulations, ratings board(s), service(s), or other organizations (each a "Ratings Board") for any video, television, gaming or other content

offered in Your Licensed Application for each locality in the Territory. Where applicable, you shall also be responsible for providing any content restriction tools or age verification functionality before enabling end-users to access mature or otherwise regulated content within Your Licensed Application.

3. Ownership and End-User Licensing and Delivery of the Licensed Applications to End Users

3.1 You acknowledge and agree that Apple, in the course of acting as agent and/or commissionaire for You, is hosting, or pursuant to Section 1.2(b) of this Schedule 1 may enable authorized third parties to host, the Licensed Application(s), and is allowing the download of those Licensed Application(s) by end-users, on Your behalf. However, You are responsible for hosting and delivering content or services sold or delivered by You using the In-App Purchase API, except for content that is included within the Licensed Application itself (i.e., the In-App Purchase simply unlocks the content) or content hosted by Apple pursuant to Section 3.3 of Attachment 2 of the Agreement. The parties acknowledge and agree that Apple shall not acquire any ownership interest in or to any of the Licensed Applications or Licensed Applications Information, and title, risk of loss, responsibility for, and control over the Licensed Applications shall, at all times, remain with You. Apple may not use any of the Licensed Applications or Licensed Application Information for any purpose, or in any manner, except as specifically authorized in the Agreement or this Schedule 1.

3.2 You may deliver to Apple Your own EULA for any Licensed Application at the time that You deliver that Licensed Application to Apple, in accordance with Section 2.1 of this Schedule 1; provided, however, that Your EULA must include and may not be inconsistent with the minimum terms and conditions specified on Exhibit B to this Schedule 1 and must comply with all applicable laws in all countries where You wish Apple to allow end-users to download that Licensed Application. Apple shall enable each end-user to review Your EULA (if any) at the time that Apple delivers that Licensed Application to that end-user, and Apple shall notify each end-user that the end-user's use of that Licensed Application is subject to the terms and conditions of Your EULA (if any). In the event that You do not furnish Your own EULA for any Licensed Application to Apple, You acknowledge and agree that each end-user's use of that Licensed Application shall be subject to Apple's standard EULA (which is part of the App Store Terms of Service).

3.3 You hereby acknowledge that the EULA for each of the Licensed Applications is solely between You and the end-user and conforms to applicable law, and Apple shall not be responsible for, and shall not have any liability whatsoever under, any EULA or any breach by You or any end-user of any of the terms and conditions of any EULA.

3.4 A Licensed Application may read or play content (magazines, newspapers, books, audio, music, video) that is offered outside of the Licensed Application (such as, by way of example, through Your website) provided that You do not link to or market external offers for such content within the Licensed Application. You are responsible for authentication access to content acquired outside of the Licensed Application.

3.5 To the extent You promote and offer in-app subscriptions, You must do so in compliance with all legal and regulatory requirements.

3.6 If Your Licensed Application is periodical content-based (e.g., magazines and newspapers), Apple may provide You with the name, email address, and zip code associated with an end-user's account when they request an auto-renewing subscription via the In-App Purchase API, provided that such user consents to the provision of data to You, and further provided that You may only use such data to promote Your own products and do so in strict compliance with Your publicly posted Privacy Policy, a copy of which must be readily viewed and

is consented to in Your Licensed Application.

4. Content Restrictions and Software Rating

4.1 You represent and warrant that: (a) You have the right to enter into this Agreement, to reproduce and distribute each of the Licensed Applications, and to authorize Apple to permit end-users to download and use each of the Licensed Applications through one or more App Stores or the Custom App Distribution Site; (b) none of the Licensed Applications, or Apple's or end-users' permitted uses of those Licensed Applications, violate or infringe any patent, copyright, trademark, trade secret or other intellectual property or contractual rights of any other person, firm, corporation or other entity and that You are not submitting the Licensed Applications to Apple on behalf of one or more third parties; (c) none of the Custom Apps, or Apple's or end-users' permitted uses of those Custom Apps, violate or infringe any patent, copyright, trademark, trade secret or other intellectual property or contractual rights of any other person, firm, corporation or other entity and that You are not submitting the Custom Apps to Apple on behalf of one or more third parties other than under license grant from one or more third parties subject to Apple's Volume Content Terms and/or Custom App Distribution; (d) each of the Licensed Applications is authorized for distribution, sale and use in, export to, and import into each of the countries designated by You under Section 2.1 of this Schedule 1, in accordance with the laws and regulations of those countries and all applicable export/import regulations; (e) none of the Licensed Applications contains any obscene, offensive or other materials that are prohibited or restricted under the laws or regulations of any of the countries You designate under Section 2.1 of this Schedule 1; (f) all information You provide using the App Store Connect tool, including any information relating to the Licensed Applications, is accurate and that, if any such information ceases to be accurate, You will promptly update it to be accurate using the App Store Connect tool; and (g) in the event a dispute arises over the content of Your Licensed Applications or use of Your intellectual property on the App Store or the Custom App Distribution Site, You agree to permit Apple to share Your contact information with the party filing such dispute and to follow Apple's app dispute process on a non-exclusive basis and without any party waiving its legal rights.

4.2 You shall use the software rating tool set forth on App Store Connect to supply information regarding each of the Licensed Applications delivered by You for marketing and fulfillment by Apple through the App Store or the Custom App Distribution Site under this Schedule 1 in order to assign a rating to each such Licensed Application. For purposes of assigning a rating to each of the Licensed Applications, You shall use Your best efforts to provide correct and complete information about the content of that Licensed Application with the software rating tool. You acknowledge and agree that Apple is relying on: (i) Your good faith and diligence in accurately and completely providing the requested information for each Licensed Application; and (ii) Your representations and warranties in Section 4.1 hereof, in making that Licensed Application available for download by end-users in each of the countries You designate hereunder. Furthermore, You authorize Apple to correct the rating of any Licensed Application of Yours that has been assigned an incorrect rating; and You agree to any such corrected rating.

4.3 In the event that any country You designate hereunder requires the approval of, or rating of, any Licensed Application by any government or industry regulatory agency as a condition for the distribution and/or use of that Licensed Application, You acknowledge and agree that Apple may elect not to make that Licensed Application available for download by end-users in that country from any App Stores or the Custom App Distribution Site.

5. Responsibility and Liability

5.1 Apple shall have no responsibility for the installation and/or use of any of the Licensed Applications by any end-user. You shall be solely responsible for any and all product warranties, end-user assistance and product support with respect to each of the Licensed Applications.

5.2 You shall be solely responsible for, and Apple shall have no responsibility or liability whatsoever with respect to, any and all claims, suits, liabilities, losses, damages, costs and expenses arising from, or attributable to, the Licensed Applications and/or the use of those Licensed Applications by any end-user, including, but not limited to: (i) claims of breach of warranty, whether specified in the EULA or established under applicable law; (ii) product liability claims; and (iii) claims that any of the Licensed Applications and/or the end-user's possession or use of those Licensed Applications infringes the copyright or other intellectual property rights of any third party.

6. Termination

6.1 This Schedule 1, and all of Apple's obligations hereunder, shall terminate upon the expiration or termination of the Agreement.

6.2 In the event that You no longer have the legal right to distribute the Licensed Applications, or to authorize Apple to allow access to those Licensed Applications by end-users, in accordance with this Schedule 1, You shall promptly notify Apple and withdraw those Licensed Applications from the App Store or the Custom App Distribution Site using the tools provided on the App Store Connect site; provided, however, that such withdrawal by You under this Section 6.2 shall not relieve You of any of Your obligations to Apple under this Schedule 1, or any liability to Apple and/or any end-user with respect to those Licensed Applications.

6.3 Apple reserves the right to cease marketing, offering, and allowing download by end-users of the Licensed Applications at any time, with or without cause, by providing notice of termination to You. Without limiting the generality of this Section 6.3, You acknowledge that Apple may cease allowing download by end-users of some or all of the Licensed Applications, or take other interim measures in Apple's sole discretion, if Apple reasonably believes that: (i) those Licensed Applications are not authorized for export to one or more of the countries designated by You under Section 2.1 hereof, in accordance with the Export Administration Regulations; (ii) those Licensed Applications and/or any end-user's possession and/or use of those Licensed Applications, infringe patent, copyright, trademark, trade secret or other intellectual property rights of any third party; (iii) the distribution and/or use of those Licensed Applications violates any applicable law in any country You designate under Section 2.1 of this Schedule 1; or (iv) You have violated the terms of the Agreement, this Schedule 1, or other documentation including without limitation the App Store Review Guidelines. An election by Apple to cease allowing download of any Licensed Applications, pursuant to this Section 6.3, shall not relieve You of Your obligations under this Schedule 1.

6.4 You may withdraw any or all of the Licensed Applications from the App Store or the Custom App Distribution Site, at any time, and for any reason, by using the tools provided on the App Store Connect site, except that, with respect to Your end-users, You hereby authorize and instruct Apple to fulfill sections 1.2(b), (c), and (d) of this Schedule 1, which shall survive termination or expiration of the Agreement unless You indicate otherwise pursuant to sections 4.1 and 6.2 of this Schedule 1.

7. Legal Consequences

The relationship between You and Apple established by this Schedule 1 may have important legal consequences for You. You acknowledge and agree that it is Your responsibility to consult with Your legal advisors with respect to Your legal obligations hereunder.

EXHIBIT A
(to Schedule 1)

1. Apple as Agent

You appoint Apple Canada, Inc. ("Apple Canada") as Your agent for the marketing and end-user download of the Licensed Applications by end-users located in the following country:

Canada

You appoint Apple Pty Limited ("APL") as Your agent for the marketing and end-user download of the Licensed Applications by end-users located in the following countries:

Australia
New Zealand

You appoint Apple Inc. as Your agent pursuant to California Civil Code §§ 2295 *et seq.* for the marketing and end-user download of the Licensed Applications by end-users located in the following countries, as updated from time to time via the App Store Connect site:*

Argentina	Cayman Islands	Guatemala	St. Kitts & Nevis
Anguilla	Chile	Honduras	St. Lucia
Antigua & Barbuda	Colombia	Jamaica	St. Vincent & The Grenadines
Bahamas	Costa Rica	Mexico	Suriname
Barbados	Dominica	Montserrat	Trinidad & Tobago
Belize	Dominican Republic	Nicaragua	Turks & Caicos
Bermuda	Ecuador	Panama	Uruguay
Bolivia	El Salvador	Paraguay	Venezuela
Brazil	Grenada	Peru	United States
British Virgin Islands	Guyana		

* Upon notice to You of the effective date by Apple, You shall appoint Apple Services LATAM LLC as Your agent pursuant to California Civil Code §§ 2295 *et seq.* for the marketing and End-User download of the Licensed Applications by End-Users located in the countries identified above, except the United States, as updated from time to time via the App Store Connect site.

You appoint iTunes KK as Your agent pursuant to Article 643 of the Japanese Civil Code for the marketing and end-user download of the Licensed Applications by end-users located in the following country:

Japan

2. Apple as Commissionaire

You appoint Apple Distribution International Ltd. as Your commissionaire for the marketing and end-user download of the Licensed Applications by end-users located in the following countries, as updated from time to time via the App Store Connect site. For the purposes of this Agreement, "commissionaire" means an agent who purports to act on his own behalf and concludes agreements in his own name but acts on behalf of other persons, as generally recognized in many Civil Law legal systems

Afghanistan	Gabon	Malawi	Saudi Arabia

Albania	Gambia	Malaysia	Senegal
Algeria	Georgia	Maldives	Serbia
Angola	Germany	Mali	Seychelles
Armenia	Ghana	Malta, Republic of	Sierra Leone
Austria	Greece	Mauritania	Singapore
Azerbaijan	Guinea-Bissau	Mauritius	Slovakia
Bahrain	Hong Kong	Micronesia, Fed States of	Slovenia
Belarus	Hungary	Moldova	Solomon Islands
Belgium	Iceland	Mongolia	South Africa
Benin	India	Montenegro	Spain
Bhutan	Indonesia	Morocco	Sri Lanka
Bosnia and Herzegovina	Iraq	Mozambique	Swaziland
Botswana	Ireland	Myanmar	Sweden
Brunei	Israel	Namibia	Switzerland
Bulgaria	Italy	Nauru	Taiwan
Burkina-Faso	Jordan	Nepal	Tajikistan
Cambodia	Kazakhstan	Netherlands	Tanzania
Cameroon	Kenya	Niger	Thailand
Cape Verde	Korea	Nigeria	Tonga
Chad	Kosovo	Norway	Tunisia
China	Kuwait	Oman	Turkey
Congo (Democratic Republic of)	Kyrgyzstan	Pakistan	Turkmenistan
Congo (Republic of)	Laos	Palau	UAE
Cote d'Ivoire	Latvia	Papua New Guinea	Uganda
Croatia	Lebanon	Philippines	Ukraine
Cyprus	Liberia	Poland	United Kingdom
Czech Republic	Libya	Portugal	Uzbekistan
Denmark	Lithuania	Qatar	Vanuatu
Egypt	Luxembourg	Romania	Vietnam
Estonia	Macau	Russia	Yemen
Fiji	Macedonia	Rwanda	Zambia
Finland	Madagascar	Sao Tome e Principe	Zimbabwe
France			

EXHIBIT B
(to Schedule 1)
Instructions for Minimum Terms of Developer's End-User License Agreement

1. Acknowledgement: You and the end-user must acknowledge that the EULA is concluded between You and the end-user only, and not with Apple, and You, not Apple, are solely responsible for the Licensed Application and the content thereof. The EULA may not provide for usage rules for Licensed Applications that are in conflict with, the App Store Terms of Service as of the Effective Date (which You acknowledge You have had the opportunity to review).

2. Scope of License: The license granted to the end-user for the Licensed Application must be limited to a non-transferable license to use the Licensed Application on any Apple-branded Products that the end-user owns or controls and as permitted by the Usage Rules set forth in the App Store Terms of Service, except that such Licensed Application may be accessed, acquired, and used by other accounts associated with the purchaser via Family Sharing or volume purchasing.

3. Maintenance and Support: You must be solely responsible for providing any maintenance and support services with respect to the Licensed Application, as specified in the EULA, or as required under applicable law. You and the end-user must acknowledge that Apple has no obligation whatsoever to furnish any maintenance and support services with respect to the Licensed Application.

4. Warranty: You must be solely responsible for any product warranties, whether express or implied by law, to the extent not effectively disclaimed. The EULA must provide that, in the event of any failure of the Licensed Application to conform to any applicable warranty, the end-user may notify Apple, and Apple will refund the purchase price for the Licensed Application to that end-user; and that, to the maximum extent permitted by applicable law, Apple will have no other warranty obligation whatsoever with respect to the Licensed Application, and any other claims, losses, liabilities, damages, costs or expenses attributable to any failure to conform to any warranty will be Your sole responsibility.

5. Product Claims: You and the end-user must acknowledge that You, not Apple, are responsible for addressing any claims of the end-user or any third party relating to the Licensed Application or the end-user's possession and/or use of that Licensed Application, including, but not limited to: (i) product liability claims; (ii) any claim that the Licensed Application fails to conform to any applicable legal or regulatory requirement; and (iii) claims arising under consumer protection or similar legislation. The EULA may not limit Your liability to the end-user beyond what is permitted by applicable law.

6. Intellectual Property Rights: You and the end-user must acknowledge that, in the event of any third party claim that the Licensed Application or the end-user's possession and use of that Licensed Application infringes that third party's intellectual property rights, You, not Apple, will be solely responsible for the investigation, defense, settlement and discharge of any such intellectual property infringement claim.

7. Legal Compliance: The end-user must represent and warrant that (i) he/she is not located in a country that is subject to a U.S. Government embargo, or that is on Title 15, Part 740 Supplement 1 Country Group E of the U.S. Code of Federal Regulations; and (ii) he/she is not listed on any U.S. Government list of prohibited or restricted parties.

8. Developer Name and Address: You must state in the EULA Your name and address, and the contact information (telephone number; E-mail address) to which any end-user questions,

complaints or claims with respect to the Licensed Application should be directed.

9. Third Party Terms of Agreement: You must state in the EULA that the end-user must comply with applicable third party terms of agreement when using Your Application, e.g., if You have a VoIP application, then the end-user must not be in violation of their wireless data service agreement when using Your Application.

10. Third Party Beneficiary: You and the end-user must acknowledge and agree that Apple, and Apple's subsidiaries, are third party beneficiaries of the EULA, and that, upon the end-user's acceptance of the terms and conditions of the EULA, Apple will have the right (and will be deemed to have accepted the right) to enforce the EULA against the end-user as a third party beneficiary thereof.

EXHIBIT C
(to Schedule 1)
App Store Promo Code Terms

Notwithstanding any other provisions of the Agreement or this Schedule 1, You hereby agree that the following terms shall apply to all promotional Custom Codes requested by You via the App Store Connect tool. For the purposes of this Exhibit C, "You" shall include additional members of Your App Store Connect team (e.g. individuals in the marketing and technical roles).

Except as otherwise expressed in writing herein, nothing in this Exhibit C shall be construed to modify the Agreement or this Schedule 1 in any way, and all capitalized terms not defined below shall have the meanings set forth in the Program Agreement.

1. DEFINITIONS:

"Holder" means an individual located in a Territory to whom You provide one or more Custom Codes;

"Custom Code" means a unique alphanumeric code generated and provided to You by Apple pursuant to this Exhibit C which allows a Holder who is an App Store customer to download or access for free from the App Store the Licensed Application for which You have requested such code via the App Store Connect tool, whether offered for free or for a fee on the App Store (the "Promo Content"); and

"Effective Period" means the period between the Custom Code Activation Date and the Custom Code Expiration Date.

2. AUTHORIZATION AND OBLIGATIONS: You hereby authorize and instruct Apple to provide You with Custom Codes upon request, pursuant to the terms of this Exhibit C, and You take full responsibility for ensuring that any team member that requests such codes shall abide by the terms of this Exhibit C. You shall be responsible for securing all necessary licenses and permissions relating to use of the Custom Codes and the Licensed Application, including any uses by You of the name(s) or other indicia of the Licensed Application, or name(s) or likenesses of the person(s) performing or otherwise featured in the Licensed Application, in any advertising, marketing, or other promotional materials, in any and all media. Apple reserves the right to request and receive copies of such licenses and permissions from You, at any time, during the Effective Period.

3. NO PAYMENT: Except for Your obligations set forth in Section 10 of this Exhibit C, You are not obligated to pay Apple any commission for the Custom Codes.

4. DELIVERY: Upon request by You via the App Store Connect tool, Apple shall provide the Custom Codes electronically to You via App Store Connect, email, or other method as may be indicated by Apple.

5. CUSTOM CODE ACTIVATION DATE: Custom Codes will become active for use by Holders upon delivery to You.

6. CUSTOM CODE EXPIRATION DATE: All unused Custom Codes, whether or not applied to an Apple ID, expire at midnight 11:59 PT on the earlier of: (a) the date that is twenty-eight (28) days after the delivery of the Custom Codes; or (b) the termination of the Agreement.

7. PERMITTED USE: You may distribute the Custom Codes until that date which is ten (10) calendar days prior to the Custom Code Expiration Date solely for the purpose of offering instances of the app for media review or promotional purposes. You may not distribute the

Custom Codes to Holders in any Territory in which You are not permitted to sell or distribute Your Licensed Application.

8. ADDITIONAL MATERIALS: Apple shall not be responsible for developing and producing any materials in relation to the Custom Codes other than the Custom Codes themselves.

9. REPRESENTATIONS, WARRANTIES, AND INDEMNIFICATION: You represent and warrant that: (i) You own or control all rights necessary to make the grant of rights, licenses, and permissions listed in Section 2, and that the exercise of such rights, licenses, and permissions shall not violate or infringe the rights of any third party, and (ii) any use of the Custom Codes shall be in accordance with the terms of this Exhibit C and shall not infringe any third party rights or violate any applicable laws, directives, rules, and regulations of any governmental authority in the Territory or anywhere else in the world. You agree to indemnify and hold Apple, its subsidiaries and affiliates (and their respective directors, officers, and employees) harmless from all losses, liabilities, damages, or expenses (including reasonable attorneys' fees and costs) resulting from any claims, demands, actions, or other proceedings arising from a breach of the representations and warranties set for h in this Section, or a breach of any other term of the Agreement and this Schedule 1.

10. PAYMENT WAIVER: You hereby waive any right to collect any royalties, proceeds, or remuneration for the distribution and download of the Licensed Application via the Custom Codes, regardless of whether any remuneration would otherwise be payable under the Agreement, including Schedule 1 thereto, if applicable. The parties acknowledge that, as between Apple and You, the parties' respective responsibilities for the payment of any royalties or other similar payments to third parties with respect to distribution and download of the Licensed Application via the Custom Codes shall be as set forth in the Agreement.

11. TERMS AND CONDITIONS: You further agree to the following terms:

(a) You shall not sell the Custom Codes or accept any form of payment, trade-in-kind, or other compensation in connection with the distribution of the Custom Codes and You shall prohibit third parties from doing so.

(b) Nothing in this Exhibit C shall cause the parties to become partners, joint venturers or co-owners, nor shall either party constitute an agent, employee, or representative of the other, or empower the other party to act for, bind, or otherwise create or assume any obligation on its behalf, in connection with any transaction under this Exhibit C; provided, however, that nothing in this Section 11(b) shall affect, impair, or modify either of the Parties' respective rights and obligations, including the agency or commissionaire relationship between them under Schedules 1, 2, and 3 of the Agreement.

(c) You shall prominently disclose any content age restrictions or warnings legally required in the Territories and ensure that Custom Codes are distributed only to persons of an age appropriate and consistent with the App Store rating for the associated Licensed Application.

(d) You shall conduct Yourself in an honest and ethical manner and shall not make any statement, orally or in writing, or do any act or engage in any activity that is obscene, unlawful, or encourages unlawful or dangerous conduct, or that may disparage, denigrate, or be detrimental to Apple or its business.

(e) Apple shall not be responsible for providing any technical or customer support to You or Holders above what Apple provides to standard or ordinary App Store users.

(f) You agree to the additional Custom Code Terms and Conditions attached hereto as Attachment 1.

(g) YOU SHALL INCLUDE THE COUNTRY SPECIFIC CODE USER TERMS AS WELL AS THE EXPIRATION DATE OF THE CUSTOM CODE ON ANY INSTRUMENT USED TO DISTRIBUTE THE CUSTOM CODE TO HOLDERS (E.G. CERTIFICATE, CARD, EMAIL, ETC). YOU SHALL RECEIVE AN EMAIL WITH THIS INFORMATION LOCALIZED FOR EACH TERRITORY UPON REQUESTING THE CUSTOM CODES IN THE APP STORE CONNECT TOOL.

Code expires on [date] and is redeemable only on the App Store for [territory]. Requires an iTunes account, subject to prior acceptance of license and usage terms. Compatible software and hardware, and internet access (fees may apply) required. Not for resale. Full terms apply; see [www.apple.com/legal/internet-services/us/terms.html]. For more information, see www.apple.com/support/ In-app purchases sold separately. This app is provided to You by [Developer's name].

(h) You shall be solely responsible for Your use of the Custom Codes, including any use by other members of Your App Store Connect team, and for any loss or liability to You or Apple therefrom.

(i) In the event Your Licensed Application is removed from the App Store for any reason, You agree to cease distribution of the Custom Codes and that Apple may deactivate such Custom Codes.

(j) You agree that Apple shall have the right to deactivate the Custom Codes, even if already delivered to Holders, in the event You violate any of the terms of this Exhibit C, the Agreement, or Schedules 1, 2, or 3 thereto.

(k) You may distribute the Custom Codes within the Territories, but agree that You shall not export any Custom Code for use outside the Territories nor represent that You have the right or ability to do so. Risk of loss and transfer of title for the Custom Codes pass to You upon delivery to You within App Store Connect, via email, or other method provided by Apple.

12. APPLE TRADEMARKS: Your use of Apple trademarks in connection with the Custom Codes is limited only to "iTunes" and "App Store" (the "Marks") subject to the following and any additional guidelines Apple may issue from time to time:

(a) You may use the Marks only during the Effective Period

(b) You shall submit any advertising, marketing, promotional or other materials, in any and all media now known or hereinafter invented, incorporating the Marks to Apple prior to use for written approval. Any such materials not expressly approved in writing by Apple shall be deemed disapproved by Apple.

(c) You may only use the Marks in a referential manner and may not use the Marks as the most prominent visual element in any materials. Your company name, trademark(s), or service mark(s) should be significantly larger than any reverence to the Marks.

(d) You may not directly or indirectly suggest Apple's sponsorship, affiliation, or endorsement of You, Your Licensed Applications, or any promotional activities for which You are requesting the Custom Codes.

(e) You acknowledge that the Marks are the exclusive property of Apple and agree not to claim any right, title, or interest in or to the Marks or at any time challenge or attack Apple's rights in the Marks. Any goodwill resulting from Your use of the Marks shall inure solely to the benefit of Apple and shall not create any right, title, or interest for You in the Marks.

13. GOVERNING LAW: Any litigation or other dispute resolution between You and Apple arising out of or relating to this Exhibit C or facts relating thereto shall be governed by Section 14.10 of the Agreement.

Attachment 1
(to Exhibit C of Schedule 1)
Custom Code Terms and Conditions

1. All Custom Codes delivered pursuant to this Exhibit C, whether or not applied to an App Store account, expire as indicated in this Exhibit C.

2. Custom Codes, and unused balances, are not redeemable for cash and cannot be returned for a cash refund, exchanged, or used to purchase any other merchandise, or provide allowances or iTunes Gifts by either You or Holder. This includes Custom Codes that have expired unused.

3. Custom Codes may only be redeemed through the App Store in the Territory, open only to persons in the Territory with a valid Apple ID. Not all App Store products may be available in all Territories. Internet access (fees may apply), the latest version of iTunes software, and other compatible software and hardware are required.

4. Access to, redemption of Custom Codes on, or purchases from, and use of products purchased on, the App Store, are subject to acceptance of its Terms of Service presented at the time of redemption or purchase, and found at http://www.apple.com/legal/itunes/ww/.

5. Latest version of iTunes software required to access the App Store, and can be downloaded at no charge at www.apple.com/itunes/download/. Use of iTunes software is subject to acceptance of its software license agreement presented at the time of installation. The minimum system requirements for running the software are available at www.apple.com/itunes/download/.

6. Custom Codes will be placed in the Holder's applicable iTunes account and are not transferable.

7. If a Holder's order exceeds the amount available on the Custom Codes, Holder must establish an iTunes Store Purchaser account and pay for the balance with a credit card.

8. Except as stated otherwise, data collection and use are subject to Apple's Privacy Policy, which can be found at http://www.apple.com/legal/privacy.

9. Apple is not responsible for lost or stolen Custom Codes. If Holders have any questions, they may visit Apple's iTunes Store Purchaser Service at www.apple.com/support/itunes/.

10. Apple reserves the right to close Holder accounts and request alternative forms of payment if Custom Codes are fraudulently obtained or used on the App Store.

11. APPLE AND ITS LICENSEES, AFFILIATES, AND LICENSORS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, WITH RESPECT TO CUSTOM CODES OR THE APP STORE, INCLUDING WITHOUT LIMITATION, ANY EXPRESS OR IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. IN THE EVENT A CUSTOM CODE IS NON-FUNCTIONAL, HOLDER'S OR COMPANY'S SOLE REMEDY, AND APPLE'S SOLE LIABILITY, SHALL BE THE REPLACEMENT OF SUCH CUSTOM CODE. THESE LIMITATIONS MAY NOT APPLY. CERTAIN LOCAL AND TERRITORY LAWS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES OR THE EXCLUSION OR LIMITATION OF CERTAIN DAMAGES. IF THESE LAWS APPLY, SOME OR ALL OF THE ABOVE DISCLAIMERS, EXCLUSIONS, OR LIMITATIONS MAY NOT APPLY, AND YOU OR HOLDER MAY ALSO HAVE ADDITIONAL RIGHTS.

12. Apple reserves the right to change any of the terms and conditions set forth in this Attachment 1 from time to time without notice.

13. Any part of these terms and conditions may be void where prohibited or restricted by law.

EXHIBIT D
(to Schedule 1)
Additional App Store Terms

1. Discoverability on the App Store: The discoverability of Your Licensed Application in the App Store depends on several factors, and Apple is under no obligation to display, feature, or rank Your Licensed Application in any particular manner or order in the App Store.

(a) The main parameters used for app ranking and discoverability are text relevance, such as using an accurate title, adding relevant keywords/metadata, and selecting descriptive categories in the Licensed Application; customer behavior relating to the number and quality of ratings and reviews and application downloads; date of launch in the App Store may also be considered for relevant searches; and whether You have violated any rules promulgated by Apple. These main parameters deliver the most relevant results to customer search queries.

(b) When considering apps to feature in the App Store, our editors look for high-quality apps across all categories, with a particular focus on new apps and apps with significant updates. The main parameters that our editors consider are UI design, user experience, innovation and uniqueness, localizations, accessibility, App Store product page screenshots, app previews, and descriptions; and additionally for games, gameplay, graphics and performance, audio, narrative and story depth, ability to replay, and gameplay controls. These main parameters showcase high-quality, well-designed, and innovative apps.

(c) If You use an Apple service for paid promotion of Your app on the App Store, Your app may be presented in a promotional placement on the Search results page and designated as advertising content.

To learn more about app discoverability, visit https://developer.apple.com/app-store/discoverability/.

2. Access to App Store Data

You can access data concerning your Licensed Application's financial performance and user engagement in App Store Connect by using App Analytics, Sales and Trends, and Payments and Financial Reports. Specifically, You can obtain all of Your Licensed Application's financial results for individual app sales and in-app purchases (including subscriptions) in Sales and Trends, or download the data from Financial Reports; and You can view App Analytics for non-personally identifiable data that allows You to understand how consumers engage with your Licensed Applications. More information can be found at https://developer.apple.com/app-store/measuring-app-performance/. App Analytics data is provided only with the consent of our customers. For more information, see https://developer.apple.com/app-store-connect/analytics/. Apple does not provide You with access to personal or other data provided by or generated through use of the App Store by other developers; nor does Apple provide other developers with access to personal or other data provided by or generated through Your use of the App Store. Such data sharing would conflict with Apple's Privacy Policy, and with our customers' expectations about how Apple treats their data. You can seek to collect information from customers directly, so long as such information is collected in a lawful manner, and You follow the App Store Review Guidelines.

Apple handles personal and non-personal information as outlined in Apple's Privacy Policy. Information about Apple's access to and practices concerning developer and customer data can be found in "App Store & Privacy," accessible at https://support.apple.com/en-us/HT210584. Apple may provide some non-personal information to strategic partners that work with Apple to provide our products and services, help Apple market to customers, and sell ads on Apple's behalf to display in the App Store and Apple News and Stocks. Such partners are obligated to protect that information and may be located wherever Apple operates.

3. P2B Regulation Complaints and Mediation for EU

These provisions become effective 12 July 2020.

Developers established in, and which offer goods or services to customer located in, the European Union may submit complaints pursuant to the Regulation of the European Parliament and of the Council on promoting fairness and transparency for business users of online intermediation services ("P2B Regulation") related to the following issues at developer.apple.com/contact: (a) Apple's alleged non-compliance with any obligations set forth in the P2B Regulation which affect You in the European Union; (b) technological issues relating directly to distribution of Your Licensed Application on the App Store in the European Union that affect You; or (c) measures taken by or behavior of Apple relating directly to distribution of Your Licensed Application on the App Store in the European Union that affect You. Apple will consider and process such complaints and communicate the outcome to You.

Pursuant to the P2B Regulation, Apple identifies the following panel of mediators with which Apple is willing to engage to attempt to reach an agreement with developers established in, and which offer goods or services to customer located in, the European Union on the settlement, out of court, of any disputes between Apple and You arising in relation to the provision of the App Store services concerned, including complaints that could not be resolved by means of our complaint-handling system:

Centre for Effective Dispute Resolution
P2B Panel of Mediators
70 Fleet Street
London
EC4Y 1EU
United Kingdom
https://www.cedr.com/p2bmediation/

Exhibit B

App Store Review Guidelines

Apps are changing the world, enriching people's lives, and enabling developers like you to innovate like never before. As a result, the App Store has grown into an exciting and vibrant ecosystem for millions of developers and more than a billion users. Whether you are a first time developer or a large team of experienced programmers, we are excited that you are creating apps for the App Store and want to help you understand our guidelines so you can be confident your app will get through the review process quickly.

Introduction
Before You Submit
1. Safety
2. Performance
3. Business
4. Design
5. Legal
After You Submit

Introduction

The guiding principle of the App Store is simple - we want to provide a safe experience for users to get apps and a great opportunity for all developers to be successful. We do this by offering a highly curated App Store where every app is reviewed by experts and an editorial team helps users discover new apps every day. For everything else there is always the open Internet. If the App Store model and guidelines are not best for your app or business idea that's okay, we provide Safari for a great web experience too.

On the following pages you will find our latest guidelines arranged into five clear sections: Safety, Performance, Business, Design, and Legal. The App Store is always changing and improving to keep up with the needs of our customers and our products. Your apps should change and improve as well in order to stay on the App Store.

A few other points to keep in mind:

- We have lots of kids downloading lots of apps. Parental controls work great to protect kids, but you have to do your part too. So know that we're keeping an eye out for the kids.
- The App Store is a great way to reach hundreds of millions of people around the world. If you build an app that you just want to show to family and friends, the App Store isn't the best way to do that. Consider using Xcode to install your app on a device for free or use Ad Hoc distribution available to Apple Developer Program members. If you're just getting started, learn more about the Apple Developer Program.
- We strongly support all points of view being represented on the App Store, as long as the apps are respectful to users with differing opinions and the quality of the app experience is great. We will reject apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it". And we think that you will also know it when you cross it.
- If you attempt to cheat the system (for example, by trying to trick the review process, steal user data, copy another developer's work, manipulate ratings or App Store discovery) your apps will be removed from the store and you will be expelled from the Developer Program.

- You are responsible for making sure everything in your app complies with these guidelines, including ad networks, analytics services, and third-party SDKs, so review and choose them carefully.
- Some features and technologies that are not generally available to developers may be offered as an entitlement for limited use cases. For example, we offer entitlements for CarPlay Audio, HyperVisor, and Privileged File Operations. Review our documentation on developer.apple.com to learn more about entitlements.

We hope these guidelines help you sail through the App Review process, and that approvals and rejections remain consistent across the board. This is a living document; new apps presenting new questions may result in new rules at any time. Perhaps your app will trigger this. We love this stuff too, and honor what you do. We're really trying our best to create the best platform in the world for you to express your talents and make a living, too.

Before You Submit

To help your app approval go as smoothly as possible, review the common missteps listed below that can slow down the review process or trigger a rejection. This doesn't replace the guidelines or guarantee approval, but making sure you can check every item on the list is a good start. If your app no longer functions as intended or you're no longer actively supporting it, it will be removed from the App Store. Learn more about App Store Improvements.

Make sure you:

- Test your app for crashes and bugs
- Ensure that all app information and metadata is complete and accurate
- Update your contact information in case App Review needs to reach you
- Provide an active demo account and login information, plus any other hardware or resources that might be needed to review your app (e.g. login credentials or a sample QR code)
- Enable backend services so that they're live and accessible during review
- Include detailed explanations of non-obvious features and in-app purchases in the App Review notes, including supporting documentation where appropriate.
- Check whether your app follows guidance in other documentation, such as:

  Development Guidelines

  UIKit
  AppKit
  WatchKit
  App Extension Programming Guide
  iOS Data Storage Guidelines
  macOS File System Documentation
  Safari App Extensions
  App Store Connect Help

  Design Guidelines

  Human Interface Guidelines

  Brand and Marketing Guidelines

Marketing Resources and Identity Guidelines

Apple Pay Identity Guidelines

Add to Apple Wallet Guidelines

Guidelines for Using Apple Trademarks and Copyrights

---

1. Safety

When people install an app from the App Store, they want to feel confident that it's safe to do so—that the app doesn't contain upsetting or offensive content, won't damage their device, and isn't likely to cause physical harm from its use. We've outlined the major pitfalls below, but if you're looking to shock and offend people, the App Store isn't the right place for your app.

1.1 Objectionable Content
Apps should not include content that is offensive, insensitive, upsetting, intended to disgust, in exceptionally poor taste, or just plain creepy. Examples of such content include:

1.1.1 Defamatory, discriminatory, or mean-spirited content, including references or commentary about religion, race, sexual orientation, gender, national/ethnic origin, or other targeted groups, particularly if the app is likely to humiliate, intimidate, or harm a targeted individual or group. Professional political satirists and humorists are generally exempt from this requirement.

1.1.2 Realistic portrayals of people or animals being killed, maimed, tortured, or abused, or content that encourages violence. "Enemies" within the context of a game cannot solely target a specific race, culture, real government, corporation, or any other real entity.

1.1.3 Depictions that encourage illegal or reckless use of weapons and dangerous objects, or facilitate the purchase of firearms or ammunition.

1.1.4 Overtly sexual or pornographic material, defined by Webster's Dictionary as "explicit descriptions or displays of sexual organs or activities intended to stimulate erotic rather than aesthetic or emotional feelings."

1.1.5 Inflammatory religious commentary or inaccurate or misleading quotations of religious texts.

1.1.6 False information and features, including inaccurate device data or trick/joke functionality, such as fake location trackers. Stating that the app is "for entertainment purposes" won't overcome this guideline. Apps that enable anonymous or prank phone calls or SMS/MMS messaging will be rejected.

1.2 User Generated Content
Apps with user-generated content present particular challenges, ranging from intellectual property infringement to anonymous bullying. To prevent abuse, apps with user-generated content or social networking services must include:

- A method for filtering objectionable material from being posted to the app
- A mechanism to report offensive content and timely responses to concerns
- The ability to block abusive users from the service
- Published contact information so users can easily reach you

Apps with user-generated content or services that end up being used primarily for pornographic content, Chatroulette-style experiences, objectification of real people (e.g. "hot-or-not" voting), making physical threats, or bullying do not belong on the App Store and may be removed without notice. If your app includes user-generated content from a web-based service, it may display incidental mature "NSFW" content, provided that the content is hidden by default and only displayed when the user turns it on via your website.

1.3 Kids Category
The Kids Category is a great way for people to easily find apps that are designed for children. If you want to participate in the Kids Category, you should focus on creating a great experience specifically for younger users. These apps must not include links out of the app, purchasing opportunities, or other distractions to kids unless reserved for a designated area behind a parental gate. Keep in mind that once customers expect your app to follow the Kids Category requirements, it will need to continue to meet these guidelines in subsequent updates, even if you decide to deselect the category. Learn more about parental gates.

You must comply with applicable privacy laws around the world relating to the collection of data from children online. Be sure to review the Privacy section of these guidelines for more information. In addition, Kids Category apps may not send personally identifiable information or device information to third parties. Apps in the Kids Category should not include third-party analytics or third-party advertising. This provides a safer experience for kids. In limited cases, third-party analytics may be permitted provided that the services do not collect or transmit the IDFA or any identifiable information about children (such as name, date of birth, email address), their location, or their devices. This includes any device, network, or other information that could be used directly or combined with other information to identify users and their devices. Third-party contextual advertising may also be permitted in limited cases provided that the services have publicly documented practices and policies for Kids Category apps that include human review of ad creatives for age appropriateness.

1.4 Physical Harm
If your app behaves in a way that risks physical harm, we may reject it. For example:

1.4.1 Medical apps that could provide inaccurate data or information, or that could be used for diagnosing or treating patients may be reviewed with greater scrutiny.

- Apps must clearly disclose data and methodology to support accuracy claims relating to health measurements, and if the level of accuracy or methodology cannot be validated, we will reject your app. For example, apps that claim to take x-rays, measure blood pressure, body temperature, blood glucose levels, or blood oxygen levels using only the sensors on the device are not permitted.
- Apps should remind users to check with a doctor in addition to using the app and before making medical decisions.

If your medical app has received regulatory clearance, please submit a link to that documentation with your app.

1.4.2 Drug dosage calculators must come from the drug manufacturer, a hospital, university, health insurance company, pharmacy or other approved entity, or receive approval by the FDA or one of its international counterparts. Given the potential harm to patients, we need to be sure that the app will be supported and updated over the long term.

1.4.3 Apps that encourage consumption of tobacco and vape products, illegal drugs, or excessive amounts of alcohol are not permitted on the App Store. Apps that encourage minors to consume any of these substances will be rejected. Facilitating the sale of marijuana, tobacco, or controlled substances (except for licensed pharmacies) isn't allowed.

1.4.4 Apps may only display DUI checkpoints that are published by law enforcement agencies, and should never encourage drunk driving or other reckless behavior such as excessive speed.

1.4.5 Apps should not urge customers to participate in activities (like bets, challenges, etc.) or use their devices in a way that risks physical harm to themselves or others.

1.5 Developer Information
People need to know how to reach you with questions and support issues. Make sure your app and its Support URL include an easy way to contact you; this is particularly important for apps that may be used in the classroom. Failure to include accurate and up-to-date contact information not only frustrates customers, but may violate the law in some countries. Also ensure that Wallet passes include valid contact information from the issuer and are signed with a dedicated certificate assigned to the brand or trademark owner of the pass.

1.6 Data Security
Apps should implement appropriate security measures to ensure proper handling of user information collected pursuant to the Apple Developer Program License Agreement and these Guidelines (see Guideline 5.1 for more information) and prevent its unauthorized use, disclosure, or access by third parties.

---

2. Performance

2.1 App Completeness
Submissions to App Review, including apps you make available for pre-order, should be final versions with all necessary metadata and fully functional URLs included; placeholder text, empty websites, and other temporary content should be scrubbed before submission. Make sure your app has been tested on-device for bugs and stability before you submit it, and include demo account info (and turn on your back-end service!) if your app includes a login. If you offer in-app purchases in your app, make sure they are complete, up-to-date, and visible to the reviewer, or that you explain why not in your review notes. Please don't treat App Review as a software testing service. We will reject incomplete app bundles and binaries that crash or exhibit obvious technical problems.

2.2 Beta Testing
Demos, betas, and trial versions of your app don't belong on the App Store – use TestFlight instead. Any app submitted for beta distribution via TestFlight should be intended for public distribution and should comply with the App Review Guidelines. Note, however, that apps using TestFlight cannot be distributed to testers in exchange for compensation of any kind, including as a reward for crowd-sourced funding. Significant updates to your beta build should be submitted to TestFlight App Review before being distributed to your testers. To learn more, visit the TestFlight Beta Testing.

2.3 Accurate Metadata
Customers should know what they're getting when they download or buy your app, so make sure your app description, screenshots, and previews accurately reflect the app's core experience and remember to keep them up-to-date with new versions.

2.3.1 Don't include any hidden or undocumented features in your app; your app's functionality should be clear to end-users and App Review. Similarly, you should not market your app on the App Store or offline as including content or services that it does not actually offer (e.g. iOS-based virus and malware scanners). Egregious or repeated

behavior is grounds for removal from the Developer Program. We work hard to make the App Store a trustworthy ecosystem and expect our app developers to follow suit; if you're dishonest, we don't want to do business with you.

2.3.2 If your app includes in-app purchases, make sure your app description, screenshots, and previews clearly indicate whether any featured items, levels, subscriptions, etc. require additional purchases. If you decide to promote in-app purchases on the App Store, ensure that the in-app purchase Display Name, Screenshot and Description are appropriate for a public audience, that you follow the guidance found in Promoting Your In-App Purchases, and that your app properly handles the SKPaymentTransactionObserver method so that customers can seamlessly complete the purchase when your app launches.

2.3.3 Screenshots should show the app in use, and not merely the title art, log-in page, or splash screen. They may also include text and image overlays (e.g. to demonstrate input mechanisms, such as an animated touch point or Apple Pencil) and show extended functionality on device, such as Touch Bar.

2.3.4 Previews are a great way for customers to see what your app looks like and what it does. To ensure people understand what they'll be getting with your app, previews may only use video screen captures of the app itself. Stickers and iMessage extensions may show the user experience in the Messages app. You can add narration and video or textual overlays to help explain anything that isn't clear from the video alone.

2.3.5 Select the most appropriate category for your app, and check out the App Store Category Definitions if you need help. If you're way off base, we may change the category for you.

2.3.6 Answer the age rating questions in App Store Connect honestly so that your app aligns properly with parental controls. If your app is mis-rated, customers might be surprised by what they get, or it could trigger an inquiry from government regulators. If your app includes media that requires the display of content ratings or warnings (e.g. films, music, games, etc.), you are responsible for complying with local requirements in each territory where your app is available.

2.3.7 Choose a unique app name, assign keywords that accurately describe your app, and don't try to pack any of your metadata with trademarked terms, popular app names, or other irrelevant phrases just to game the system. App names must be limited to 30 characters and should not include prices, terms, or descriptions that are not the name of the app. App subtitles are a great way to provide additional context for your app; they must follow our standard metadata rules and should not include inappropriate content, reference other apps, or make unverifiable product claims. Apple may modify inappropriate keywords at any time or take other appropriate steps to prevent abuse.

2.3.8 Metadata should be appropriate for all audiences, so make sure your app and in-app purchase icons, screenshots, and previews adhere to a 4+ age rating even if your app is rated higher. For example, if your app is a game that includes violence, select images that don't depict a gruesome death or a gun pointed at a specific character. Use of terms like "For Kids" and "For Children" in app metadata is reserved for the Kids Category. Remember to ensure your metadata, including app name and icons (small, large, Apple Watch app, alternate icons, etc.), are similar to avoid creating confusion.

2.3.9 You are responsible for securing the rights to use all materials in your app icons, screenshots, and previews, and you should display fictional account information instead of data from a real person.

2.3.10 Make sure your app is focused on the iOS, Mac, Apple TV or Apple Watch experience, and don't include names, icons, or imagery of other mobile platforms in your app or metadata, unless there is specific, approved interactive functionality. Make sure

your app metadata is focused on the app itself and its experience. Don't include irrelevant information, including but not limited to information about Apple or the development process.

2.3.11 Apps you submit for pre-order on the App Store must be complete and deliverable as submitted. Ensure that the app you ultimately release is not materially different from what you advertise while the app is in a pre-order state. If you make material changes to the app (e.g. change business models), you should restart your pre-order sales.

2.3.12 Apps must clearly describe new features and product changes in their "What's New" text. Simple bug fixes, security updates, and performance improvements may rely on a generic description, but more significant changes must be listed in the notes.

2.4 Hardware Compatibility

2.4.1 To ensure people get the most out of your app, iPhone apps should run on iPad whenever possible. We encourage you to consider building universal apps so customers can use them on all of their devices. Learn more about Universal apps.

2.4.2 Design your app to use power efficiently and be used in a way that does not risk damage to the device. Apps should not rapidly drain battery, generate excessive heat, or put unnecessary strain on device resources. For example, apps should not encourage placing the device under a mattress or pillow while charging or perform excessive write cycles to the solid state drive. Apps, including any third-party advertisements displayed within them, may not run unrelated background processes, such as cryptocurrency mining.

2.4.3 People should be able to use your Apple TV app without the need for hardware inputs beyond the Siri remote or third-party game controllers, but feel free to provide enhanced functionality when other peripherals are connected. If you require a game controller, make sure you clearly explain that in your metadata so customers know they need additional equipment to play.

2.4.4 Apps should never suggest or require a restart of the device or modifications to system settings unrelated to the core functionality of the application. For example, don't encourage users to turn off Wi-Fi, disable security features, etc.

2.4.5 Apps distributed via the Mac App Store have some additional requirements to keep in mind:

(i) They must be appropriately sandboxed, and follow macOS File System Documentation. They should also only use the appropriate macOS APIs for modifying user data stored by other Apps (e.g. bookmarks, Address Book, or Calendar entries).

(ii) They must be packaged and submitted using technologies provided in Xcode; no third-party installers allowed. They must also be self-contained, single application installation bundles and cannot install code or resources in shared locations.

(iii) They may not auto-launch or have other code run automatically at startup or login without consent nor spawn processes that continue to run without consent after a user has quit the app. They should not automatically add their icons to the Dock or leave short cuts on the user desktop.

(iv) They may not download or install standalone apps, kexts, additional code, or resources to add functionality or significantly change the app from what we see during the review process.

(v) They may not request escalation to root privileges or use setuid attributes.

(vi) They may not present a license screen at launch, require license keys, or implement their own copy protection.

(vii) They must use the Mac App Store to distribute updates; other update mechanisms are not allowed.

(viii) Apps should run on the currently shipping OS and may not use deprecated or optionally installed technologies (e.g. Java, Rosetta)

(ix) Apps must contain all language and localization support in a single app bundle.

2.5 Software Requirements

2.5.1 Apps may only use public APIs and must run on the currently shipping OS. Learn more about public APIs. Keep your apps up-to-date and make sure you phase out any deprecated features, frameworks or technologies that will no longer be supported in future versions of an OS. Apps should use APIs and frameworks for their intended purposes and indicate that integration in their app description. For example, the HomeKit framework should provide home automation services; and HealthKit should be used for health and fitness purposes and integrate with the Health app.

2.5.2 Apps should be self-contained in their bundles, and may not read or write data outside the designated container area, nor may they download, install, or execute code which introduces or changes features or functionality of the app, including other apps. Educational apps designed to teach, develop, or allow students to test executable code may, in limited circumstances, download code provided that such code is not used for other purposes. Such apps must make the source code provided by the Application completely viewable and editable by the user.

2.5.3 Apps that transmit viruses, files, computer code, or programs that may harm or disrupt the normal operation of the operating system and/or hardware features, including Push Notifications and Game Center, will be rejected. Egregious violations and repeat behavior will result in removal from the Developer Program.

2.5.4 Multitasking apps may only use background services for their intended purposes: VoIP, audio playback, location, task completion, local notifications, etc. If your app uses location background mode, include a reminder that doing so may dramatically decrease battery life.

2.5.5 Apps must be fully functional on IPv6-only networks.

2.5.6 Apps that browse the web must use the appropriate WebKit framework and WebKit Javascript.

2.5.7 Video streaming content over a cellular network longer than 10 minutes must use HTTP Live Streaming and include a baseline 192 kbps HTTP Live stream.

2.5.8 Apps that create alternate desktop/home screen environments or simulate multi-app widget experiences will be rejected.

2.5.9 Apps that alter or disable the functions of standard switches, such as the Volume Up/Down and Ring/Silent switches, or other native user interface elements or behaviors will be rejected. For example, apps should not block links out to other apps or other features that users would expect to work a certain way. Learn more about proper handling of links.

2.5.10 Apps should not be submitted with empty ad banners or test advertisements.

2.5.11 SiriKit and Shortcuts

(i) Apps integrating SiriKit and Shortcuts should only sign up for intents they can handle without the support of an additional app and that users would expect from the stated functionality. For example, if your app is a meal planning app, you should not

incorporate an intent to start a workout, even if the app shares integration with a fitness app.

(ii) Ensure that the vocabulary and phrases in your plist pertains to your app and the Siri functionality of the intents the app has registered for. Aliases must relate directly to your app or company name and should not be generic terms or include third-party app names or services.

(iii) Resolve the Siri request or Shortcut in the most direct way possible and do not insert ads or other marketing between the request and its fulfillment. Only request a disambiguation when required to complete the task (e.g. asking the user to specify a particular type of workout).

2.5.12 Apps using CallKit or including an SMS Fraud Extension should only block phone numbers that are confirmed spam. Apps that include call-, SMS-, and MMS- blocking functionality or spam identification must clearly identify these features in their marketing text and explain the criteria for their blocked and spam lists. You may not use the data accessed via these tools for any purpose not directly related to operating or improving your app or extension (e.g. you may not use, share, or sell it for tracking purposes, creating user profiles, etc.).

2.5.13 Apps using facial recognition for account authentication must use LocalAuthentication (and not ARKit or other facial recognition technology) where possible, and must use an alternate authentication method for users under 13 years old.

2.5.14 Apps must request explicit user consent and provide a clear visual and/or audible indication when recording, logging, or otherwise making a record of user activity. This includes any use of the device camera, microphone, screen recordings, or other user inputs.

2.5.15 Apps that enable users to view and select files should include items from the Files app and the user's iCloud documents.

---

3. Business

There are many ways to monetize your app on the App Store. If your business model isn't obvious, make sure to explain in its metadata and App Review notes. If we can't understand how your app works or your in-app purchases aren't immediately obvious, it will delay your review and may trigger a rejection. And while pricing is up to you, we won't distribute apps and in-app purchase items that are clear rip-offs. We'll reject expensive apps that try to cheat users with irrationally high prices.

If we find that you have attempted to manipulate reviews, inflate your chart rankings with paid, incentivized, filtered, or fake feedback, or engage with third-party services to do so on your behalf, we will take steps to preserve the integrity of the App Store, which may include expelling you from the Developer Program.

3.1 Payments

3.1.1 In-App Purchase:

- If you want to unlock features or functionality within your app, (by way of example: subscriptions, in-game currencies, game levels, access to premium content, or unlocking a full version), you must use in-app purchase. Apps may not use their own

mechanisms to unlock content or functionality, such as license keys, augmented reality markers, QR codes, etc. Apps and their metadata may not include buttons, external links, or other calls to action that direct customers to purchasing mechanisms other than in-app purchase.

- Apps may use in-app purchase currencies to enable customers to "tip" digital content providers in the app.
- Any credits or in-game currencies purchased via in-app purchase may not expire, and you should make sure you have a restore mechanism for any restorable in-app purchases.
- Remember to assign the correct purchasability type or your app will be rejected.
- Apps may enable gifting of items that are eligible for in-app purchase to others. Such gifts may only be refunded to the original purchaser and may not be exchanged.
- Apps distributed via the Mac App Store may host plug-ins or extensions that are enabled with mechanisms other than the App Store.
- Apps offering "loot boxes" or other mechanisms that provide randomized virtual items for purchase must disclose the odds of receiving each type of item to customers prior to purchase.
- Non-subscription apps may offer a free time-based trial period before presenting a full unlock option by setting up a Non-Consumable IAP item at Price Tier 0 that follows the naming convention: "XX-day Trial." Prior to the start of the trial, your app must clearly identify its duration, the content or services that will no longer be accessible when the trial ends, and any downstream charges the user would need to pay for full functionality. Learn more about managing content access and the duration of the trial period using Receipts and Device Check.

3.1.2 Subscriptions: Apps may offer auto-renewing in-app purchase subscriptions, regardless of category on the App Store. When incorporating auto-renewable subscriptions into your app, be sure to follow the guidelines below.

3.1.2(a) Permissible uses: If you offer an auto-renewing subscription, you must provide ongoing value to the customer, and the subscription period must last at least seven days and be available across all of the user's devices. While the following list is not exhaustive, examples of appropriate subscriptions include: new game levels; episodic content; multiplayer support; apps that offer consistent, substantive updates; access to large collections of, or continually updated, media content; software as a service ("SAAS"); and cloud support. In addition:

- Subscriptions may be offered alongside a la carte offerings (e.g. you may offer a subscription to an entire library of films as well the purchase or rental of a single movie).
- You may offer a single subscription that is shared across your own apps and services, but these subscriptions may not extend to third-party apps or services. Games offered in a game subscription must be owned or exclusively licensed by the developer (e.g. not part of a game publishing platform). Each game must be downloaded directly from the App Store, must be designed to avoid duplicate payment by a subscriber, and should not disadvantage non-subscriber customers.
- Subscriptions must work on all of the user's devices where the app is available. Learn more about sharing a subscription across your apps.
- Apps must not force users to rate the app, review the app, download other apps, or other similar actions in order to access functionality, content, or use of the app.

- As with all apps, those offering subscriptions should allow a user to get what they've paid for without performing additional tasks, such as posting on social media, uploading contacts, checking in to the app a certain number of times, etc.
- Subscriptions may include consumable credits, gems, in-game currencies, etc., and you may offer subscriptions that include access to discounted consumable goods (e.g. a platinum membership that exposes gem-packs for a reduced price).
- If you are changing your existing app to a subscription-based business model, you should not take away the primary functionality existing users have already paid for. For example, let customers who have already purchased a "full game unlock" continue to access the full game after you introduce a subscription model for new customers.
- Auto-renewing subscription apps may offer a free trial period to customers by providing the relevant information set forth in App Store Connect.
- Apps that attempt to scam users will be removed from the App Store. This includes apps that attempt to trick users into purchasing a subscription under false pretenses or engage in bait-and-switch and scam practices will be removed from the App Store and you may be removed from the Apple Developer Program. Learn more about Subscription Free Trials.

3.1.2(b) Upgrades and Downgrades: Users should have a seamless upgrade/downgrade experience and should not be able to inadvertently subscribe to multiple variations of the same thing. Review best practices on managing your subscription upgrade and downgrade options.

3.1.2(c) Subscription Information: Before asking a customer to subscribe, you should clearly describe what the user will get for the price. How many issues per month? How much cloud storage? What kind of access to your service? Ensure you clearly communicate the requirements described in Schedule 2 of the Apple Developer Program License Agreement, found in Agreements, Tax, and Banking.

3.1.3(a) "Reader" Apps: Apps may allow a user to access previously purchased content or content subscriptions (specifically: magazines, newspapers, books, audio, music, video, access to professional databases, VoIP, cloud storage, and approved services such as classroom management apps), provided that you agree not to directly or indirectly target iOS users to use a purchasing method other than in-app purchase, and your general communications about other purchasing methods are not designed to discourage use of in-app purchase.

3.1.3(b) Multiplatform Services: Apps that operate across multiple platforms may allow users to access content, subscriptions, or features they have acquired in your app on other platforms or your web site, including consumable items in multiplatform games, provided those items are also available as in-app purchases within the app. You must not directly or indirectly target iOS users to use a purchasing method other than in-app purchase, and your general communications about other purchasing methods must not discourage use of in-app purchase.

3.1.4 Hardware-Specific Content: In limited circumstances, such as when features are dependent upon specific hardware to function, the app may unlock that functionality without using in-app purchase (e.g. an astronomy app that adds features when synced with a telescope). App features that work in combination with an approved physical product (such as a toy) on an *optional* basis may unlock functionality without using in-app purchase, provided that an in-app purchase option is available as well. You may not, however, require users to purchase unrelated products or engage in advertising or marketing activities to unlock app functionality.

3.1.5(a) Goods and Services Outside of the App: If your app enables people to purchase goods or services that will be consumed outside of the app, you must use purchase methods other than in-app purchase to collect those payments, such as Apple Pay or traditional credit card entry.

3.1.5(b) Cryptocurrencies:

- (i) Wallets: Apps may facilitate virtual currency storage, provided they are offered by developers enrolled as an organization.
- (ii) Mining: Apps may not mine for cryptocurrencies unless the processing is performed off device (e.g. cloud-based mining).
- (iii) Exchanges: Apps may facilitate transactions or transmissions of cryptocurrency on an approved exchange, provided they are offered by the exchange itself.
- (iv) Initial Coin Offerings: Apps facilitating Initial Coin Offerings ("ICOs"), cryptocurrency futures trading, and other crypto-securities or quasi-securities trading must come from established banks, securities firms, futures commission merchants ("FCM"), or other approved financial institutions and must comply with all applicable law.
- (v) Cryptocurrency apps may not offer currency for completing tasks, such as downloading other apps, encouraging other users to download, posting to social networks, etc.

3.1.6 Apple Pay: Apps using Apple Pay must provide all material purchase information to the user prior to sale of any good or service and must use Apple Pay branding and user interface elements correctly, as described in the Apple Pay Identity Guidelines and Human Interface Guidelines. Apps using Apple Pay to offer recurring payments must, at a minimum, disclose the following information:

- The length of the renewal term and the fact that it will continue until canceled
- What will be provided during each period
- The actual charges that will be billed to the customer
- How to cancel

3.1.7 Advertising: Ads displayed in an app must be appropriate for the app's age rating, allow the user to see all information used to target them for that ad (without requiring the user to leave the app), and may not engage in targeted or behavioral advertising based on sensitive user data such as health/medical data (e.g. from the HealthKit APIs), school and classroom data (e.g. from ClassKit), or from kids (e.g. from apps in the Kids Category), etc. Interstitial ads or ads that interrupt or block the user experience must clearly indicate that they are an ad, must not manipulate or trick users into tapping into them, and must provide easily accessible and visible close/skip buttons large enough for people to easily dismiss the ad.

3.2 Other Business Model Issues

The lists below are not exhaustive, and your submission may trigger a change or update to our policies, but here are some additional dos and don'ts to keep in mind:

3.2.1 Acceptable

(i) Displaying your own apps for purchase or promotion within your app, provided the app is not merely a catalog of your apps.

(ii) Displaying or recommending a collection of third-party apps that are designed for a specific approved need (e.g. health management, aviation, accessibility). Your app should provide robust editorial content so that it doesn't seem like a mere storefront.

(iii) Disabling access to specific approved rental content (e.g. films, television programs, music, books) after the rental period has expired; all other items and services may not expire.

(iv) Wallet passes can be used to make or receive payments, transmit offers, or offer identification (such as movie tickets, coupons, and VIP credentials). Other uses may result in the rejection of the app and the revocation of Wallet credentials.

(v) Insurance apps must be free, in legal-compliance in the regions distributed, and cannot use in-app purchase.

(vi) Approved nonprofits may fundraise directly within their own apps or third-party apps, provided those fundraising campaigns adhere to all App Review Guidelines and offer Apple Pay support. These apps must disclose how the funds will be used, abide by all required local and federal laws, and ensure appropriate tax receipts are available to donors. Additional information shall be provided to App Review upon request. Nonprofit platforms that connect donors to other nonprofits must ensure that every nonprofit listed in the app has also gone through the nonprofit approval process. Learn more about becoming an approved nonprofit.

(vii) Apps may enable individual users to give a monetary gift to another individual without using in-app purchase, provided that (a) the gift is a completely optional choice by the giver, and (b) 100% of the funds go to the receiver of the gift. However, a gift that is connected to or associated at any point in time with receiving digital content or services must use in-app purchase.

(viii) Apps used for financial trading, investing, or money management should come from the financial institution performing such services or must use a public API offered by the institution in compliance with its Terms & Conditions.

3.2.2 Unacceptable

(i) Creating an interface for displaying third-party apps, extensions, or plug-ins similar to the App Store or as a general-interest collection.

(ii) Monetizing built-in capabilities provided by the hardware or operating system, such as Push Notifications, the camera, or the gyroscope; or Apple services, such as Apple Music access or iCloud storage.

(iii) Artificially increasing the number of impressions or click-throughs of ads, as well as apps that are designed predominantly for the display of ads.

(iv) Unless you are an approved nonprofit or otherwise permitted under Section 3.2.1 (vi) above, collecting funds within the app for charities and fundraisers. Apps that seek to raise money for such causes must be free on the App Store and may only collect funds outside of the app, such as via Safari or SMS.

(v) Arbitrarily restricting who may use the app, such as by location or carrier.

(vi) Apps should allow a user to get what they've paid for without performing additional tasks, such as posting on social media, uploading contacts, checking in to the app a certain number of times, etc. Apps should not require users to rate the app, review the app, watch videos, download other apps, tap on advertisements, or take other similar actions in order to access functionality, content, use the app, or receive monetary or other compensation, including but not limited to gift cards and codes.

(vii) Artificially manipulating a user's visibility, status, or rank on other services unless permitted by that service's Terms and Conditions.

(viii) Apps that facilitate binary options trading are not permitted on the App Store. Consider a web app instead. Apps that facilitate trading in contracts for difference

("CFDs") or other derivatives (e.g. FOREX) must be properly licensed in all jurisdictions where the service is available.

(ix) Apps must not force users to rate the app, review the app, download other apps, or perform other similar actions in order to access functionality, content, or use of the app.

---

4. Design

Apple customers place a high value on products that are simple, refined, innovative, and easy to use, and that's what we want to see on the App Store. Coming up with a great design is up to you, but the following are minimum standards for approval to the App Store. And remember that even after your app has been approved, you should update your app to ensure it remains functional and engaging to new and existing customers. Apps that stop working or offer a degraded experience may be removed from the App Store at any time.

4.1 Copycats
Come up with your own ideas. We know you have them, so make yours come to life. Don't simply copy the latest popular app on the App Store, or make some minor changes to another app's name or UI and pass it off as your own. In addition to risking an intellectual property infringement claim, it makes the App Store harder to navigate and just isn't fair to your fellow developers.

4.2 Minimum Functionality
Your app should include features, content, and UI that elevate it beyond a repackaged website. If your app is not particularly useful, unique, or "app-like," it doesn't belong on the App Store. If your App doesn't provide some sort of lasting entertainment value, it may not be accepted. Apps that are simply a song or movie should be submitted to the iTunes Store. Apps that are simply a book or game guide should be submitted to the Apple Books Store.

4.2.1 Apps using ARKit should provide rich and integrated augmented reality experiences; merely dropping a model into an AR view or replaying animation is not enough.

4.2.2 Other than catalogs, apps shouldn't primarily be marketing materials, advertisements, web clippings, content aggregators, or a collection of links.

4.2.3

- (i) Your app should work on its own without requiring installation of another app to function.
- (ii) Make sure you include sufficient content in the binary for the app to function at launch.
- (iii) If your app needs to download additional resources, disclose the size of the download and prompt users before doing so.

4.2.4 Apple Watch apps that appear to be a watch face are confusing, because people will expect them to work with device features such as swipes, notifications, and third-party complications. Creative ways of expressing time as an app interface is great (say, a tide clock for surfers), but if your app comes too close to resembling a watch face, we will reject it.

4.2.5 Apps that are primarily iCloud and iCloud Drive file managers need to include additional app functionality to be approved.

4.2.6 Apps created from a commercialized template or app generation service will be rejected unless they are submitted directly by the provider of the app's content. These services should not submit apps on behalf of their clients and should offer tools that let their clients create customized, innovative apps that provide unique customer experiences. Another acceptable option for template providers is to create a single binary to host all client content in an aggregated or "picker" model, for example as a restaurant finder app with separate customized entries or pages for each client restaurant, or as an event app with separate entries for each client event.

4.2.7 Remote Desktop Clients: If your remote desktop app acts as a mirror of specific software or services rather than a generic mirror of the host device, it must comply with the following:

- (a) The app must only connect to a user-owned host device that is a personal computer or dedicated game console owned by the user, and both the host device and client must be connected on a local and LAN-based network.
- (b) Any software or services appearing in the client are fully executed on the host device, rendered on the screen of the host device, and may not use APIs or platform features beyond what is required to stream the Remote Desktop.
- (c) All account creation and management must be initiated from the host device.
- (d) The UI appearing on the client does not resemble an iOS or App Store view, does not provide a store-like interface, or include the ability to browse, select, or purchase software not already owned or licensed by the user. For the sake of clarity, transactions taking place within mirrored software do not need to use in-app purchase, provided the transactions are processed on the host device.
- (e) Thin clients for cloud-based apps are not appropriate for the App Store.

4.3 Spam

Don't create multiple Bundle IDs of the same app. If your app has different versions for specific locations, sports teams, universities, etc., consider submitting a single app and provide the variations using in-app purchase. Also avoid piling on to a category that is already saturated; the App Store has enough fart, burp, flashlight, fortune telling, dating, and Kama Sutra apps, etc. already. We will reject these apps unless they provide a unique, high-quality experience. Spamming the store may lead to your removal from the Developer Program.

4.4 Extensions

Apps hosting or containing extensions must comply with the App Extension Programming Guide or the Safari App Extensions Guide and should include some functionality, such as help screens and settings interfaces where possible. You should clearly and accurately disclose what extensions are made available in the app's marketing text, and the extensions may not include marketing, advertising, or in-app purchases.

4.4.1 Keyboard extensions have some additional rules.
They must:

- Provide keyboard input functionality (e.g. typed characters);
- Follow Sticker guidelines if the keyboard includes images or emoji;
- Provide a method for progressing to the next keyboard;
- Remain functional without full network access and without requiring full access;
- Collect user activity only to enhance the functionality of the user's keyboard extension on the iOS device.

They must not:

- Launch other apps besides Settings; or
- Repurpose keyboard buttons for other behaviors (e.g. holding down the "return" key to launch the camera).

4.4.2 Safari extensions must run on the current version of Safari on macOS. They may not interfere with System or Safari UI elements and must never include malicious or misleading content or code. Violating this rule will lead to removal from the Developer Program. Safari extensions should not claim access to more websites than strictly necessary to function.

4.4.3 Stickers
Stickers are a great way to make Messages more dynamic and fun, letting people express themselves in clever, funny, meaningful ways. Whether your app contains a sticker extension or you're creating free-standing sticker packs, its content shouldn't offend users, create a negative experience, or violate the law.

(i) In general, if it wouldn't be suitable for the App Store, it doesn't belong in a sticker.

(ii) Consider regional sensitivities, and do not make your sticker pack available in a country where it could be poorly received or violate local law.

(iii) If we don't understand what your stickers mean, include a clear explanation in your review notes to avoid any delays in the review process.

(iv) Ensure your stickers have relevance beyond your friends and family; they should not be specific to personal events, groups, or relationships.

(v) You must have all the necessary copyright, trademark, publicity rights, and permissions for the content in your stickers, and shouldn't submit anything unless you're authorized to do so. Keep in mind that you must be able to provide verifiable documentation upon request. Apps with sticker content you don't have rights to use will be removed from the App Store and repeat offenders will be removed from the Developer Program. If you believe your content has been infringed by another provider, submit a claim here.

4.5 Apple Sites and Services

4.5.1 Apps may use approved Apple RSS feeds such as the iTunes Store RSS feed, but may not scrape any information from Apple sites (e.g. apple.com, the iTunes Store, App Store, App Store Connect, developer portal, etc.) or create rankings using this information.

4.5.2 Apple Music

(i) The MusicKit APIs let customers access their subscription while using your app. They are intended for simple music playback by Apple Music subscribers. Users must initiate the playback of an Apple Music stream and be able to navigate using standard media controls such as "play," "pause," and "skip." Moreover, your app may not require payment or indirectly monetize access to the Apple Music service (e.g. in-app purchase, advertising, requesting user info, etc.). Do not download, upload, or enable sharing of music files sourced from the MusicKit APIs, except as explicitly permitted in MusicKit documentation.

(ii) Using the MusicKit APIs is not a replacement for securing the licenses you might need for a deeper or more complex music integration. For example, if you want your app to play a specific song at a particular moment, or to create audio or video files that can be shared to social media, you'll need to contact rights-holders directly to get their permission (e.g. synchronization or adaptation rights) and assets. Cover art and other metadata may only be used in connection with music playback or playlists (including App Store screenshots displaying your app's functionality), and should not be used in

any marketing or advertising without getting specific authorization from rights-holders. Make sure to follow the Apple Music Identity Guidelines when integrating Apple Music services in your app.

(iii) Apps that access Apple Music user data, such as playlists and favorites, must clearly disclose this access in the purpose string. Any data collected may not be shared with third parties for any purpose other than supporting or improving the app experience. This data may not be used to identify users or devices, or to target advertising.

4.5.3 Do not use Apple Services to spam, phish, or send unsolicited messages to customers, including Game Center, Push Notifications, etc. Do not attempt to reverse lookup, trace, relate, associate, mine, harvest, or otherwise exploit Player IDs, aliases, or other information obtained through Game Center, or you will be removed from the Developer Program.

4.5.4 Push Notifications must not be required for the app to function, and should not be used to send sensitive personal or confidential information. Push Notifications should not be used for promotions or direct marketing purposes unless customers have explicitly opted in to receive them via consent language displayed in your app's UI, and you provide a method in your app for a user to opt out from receiving such messages. Abuse of these services may result in revocation of your privileges.

4.5.5 Only use Game Center Player IDs in a manner approved by the Game Center terms and do not display them in the app or to any third party.

4.5.6 Apps may use Unicode characters that render as Apple emoji in their app and app metadata. Apple emoji may not be used on other platforms or embedded directly in your app binary.

4.6 Alternate App Icons

Apps may display customized icons, for example, to reflect a sports team preference, provided that each change is initiated by the user and the app includes settings to revert to the original icon. All icon variants must relate to the content of the app and changes should be consistent across all system assets, so that the icons displayed in Settings, Notifications, etc. match the new springboard icon. This feature may not be used for dynamic, automatic, or serial changes, such as to reflect up-to-date weather information, calendar notifications, etc.

4.7 HTML5 Games, Bots, etc.

Apps may contain or run code that is not embedded in the binary (e.g. HTML5-based games, bots, etc.), as long as code distribution isn't the main purpose of the app, the code is not offered in a store or store-like interface, and provided that the software (1) is free or purchased using in-app purchase; (2) only uses capabilities available in a standard WebKit view (e.g. it must open and run natively in Safari without modifications or additional software); your app must use WebKit and JavaScript Core to run third-party software and should not attempt to extend or expose native platform APIs to third-party software; (3) is offered by developers that have joined the Apple Developer Program and signed the Apple Developer Program License Agreement; (4) does not provide access to real money gaming, lotteries, or charitable donations; (5) adheres to the terms of these App Review Guidelines (e.g. does not include objectionable content); and (6) does not offer digital goods or services for sale. Upon request, you must provide an index of software and metadata available in your app. It must include Apple Developer Program Team IDs for the providers of the software along with a URL which App Review can use to confirm that the software complies with the requirements above.

4.8 Sign in with Apple

Apps that use a third-party or social login service (such as Facebook Login, Google Sign-In, Sign in with Twitter, Sign In with LinkedIn, Login with Amazon, or WeChat Login) to set up or authenticate the user's primary account with the app must also offer Sign in with Apple as an equivalent option. A user's primary account is the account they establish with your app for the purposes of identifying themselves, signing in, and accessing your features and associated services.

Sign in with Apple is not required if:

- Your app exclusively uses your company's own account setup and sign-in systems.
- Your app is an education, enterprise, or business app that requires the user to sign in with an existing education or enterprise account.
- Your app uses a government or industry-backed citizen identification system or electronic ID to authenticate users.
- Your app is a client for a specific third-party service and users are required to sign in to their mail, social media, or other third-party account directly to access their content.

---

5. Legal

Apps must comply with all legal requirements in any location where you make them available (if you're not sure, check with a lawyer). We know this stuff is complicated, but it is your responsibility to understand and make sure your app conforms with all local laws, not just the guidelines below. And of course, apps that solicit, promote, or encourage criminal or clearly reckless behavior will be rejected. In extreme cases, such as apps that are found to facilitate human trafficking and/or the exploitation of children, appropriate authorities will be notified.

5.1 Privacy
Protecting user privacy is paramount in the Apple ecosystem, and you should use care when handling personal data to ensure you've complied with privacy best practices, applicable laws and the terms of the Apple Developer Program License Agreement, not to mention customer expectations. More particularly:

5.1.1 Data Collection and Storage

(i) Privacy Policies: All apps must include a link to their privacy policy in the App Store Connect metadata field and within the app in an easily accessible manner. The privacy policy must clearly and explicitly:

- Identify what data, if any, the app/service collects, how it collects that data, and all uses of that data.
- Confirm that any third party with whom an app shares user data (in compliance with these Guidelines) — such as analytics tools, advertising networks and third-party SDKs, as well as any parent, subsidiary or other related entities that will have access to user data — will provide the same or equal protection of user data as stated in the app's privacy policy and required by these Guidelines.
- Explain its data retention/deletion policies and describe how a user can revoke consent and/or request deletion of the user's data.

(ii) Permission Apps that collect user or usage data must secure user consent for the collection, even if such data is considered to be anonymous at the time of or immediately following collection. Paid functionality must not be dependent on or require

a user to grant access to this data. Apps must also provide the customer with an easily accessible and understandable way to withdraw consent. Ensure your purpose strings clearly and completely describe your use of the data. Apps that collect data for a legitimate interest without consent by relying on the terms of the European Union's General Data Protection Regulation ("GDPR") or similar statute must comply with all terms of that law. Learn more about Requesting Permission.

(iii) Data Minimization: Apps should only request access to data relevant to the core functionality of the app and should only collect and use data that is required to accomplish the relevant task. Where possible, use the out-of-process picker or a share sheet rather than requesting full access to protected resources like Photos or Contacts.

(iv) Access Apps must respect the user's permission settings and not attempt to manipulate, trick, or force people to consent to unnecessary data access. For example, apps that include the ability to post photos to a social network must not also require microphone access before allowing the user to upload photos. Where possible, provide alternative solutions for users who don't grant consent. For example, if a user declines to share Location, offer the ability to manually enter an address.

(v) Account Sign-In: If your app doesn't include significant account-based features, let people use it without a log-in. Apps may not require users to enter personal information to function, except when directly relevant to the core functionality of the app or required by law. If your core app functionality is not related to a specific social network (e.g. Facebook, WeChat, Weibo, Twitter, etc.), you must provide access without a login or via another mechanism. Pulling basic profile information, sharing to the social network, or inviting friends to use the app are not considered core app functionality. The app must also include a mechanism to revoke social network credentials and disable data access between the app and social network from within the app. An app may not store credentials or tokens to social networks off of the device and may only use such credentials or tokens to directly connect to the social network from the app itself while the app is in use.

(vi) Developers that use their apps to surreptitiously discover passwords or other private data will be removed from the Developer Program.

(vii) SafariViewController must be used to visibly present information to users; the controller may not be hidden or obscured by other views or layers. Additionally, an app may not use SafariViewController to track users without their knowledge and consent.

(viii) Apps that compile personal information from any source that is not directly from the user or without the user's explicit consent, even public databases, are not permitted on the App Store.

(ix) Apps that provide services in highly-regulated fields (such as banking and financial services, healthcare, and air travel) or that require sensitive user information should be submitted by a legal entity that provides the services, and not by an individual developer.

5.1.2 Data Use and Sharing

(i) Unless otherwise permitted by law, you may not use, transmit, or share someone's personal data without first obtaining their permission. You must provide access to information about how and where the data will be used. Data collected from apps may only be shared with third parties to improve the app or serve advertising (in compliance with the Apple Developer Program License Agreement). Apps that share user data without user consent or otherwise complying with data privacy laws may be removed from sale and may result in your removal from the Apple Developer Program.

(ii) Data collected for one purpose may not be repurposed without further consent unless otherwise explicitly permitted by law.

(iii) Apps should not attempt to surreptitiously build a user profile based on collected data and may not attempt, facilitate, or encourage others to identify anonymous users or reconstruct user profiles based on data collected from Apple-provided APIs or any data that you say has been collected in an "anonymized," "aggregated," or otherwise non-identifiable way.

(iv) Do not use information from Contacts, Photos, or other APIs that access user data to build a contact database for your own use or for sale/distribution to third parties, and don't collect information about which other apps are installed on a user's device for the purposes of analytics or advertising/marketing.

(v) Do not contact people using information collected via a user's Contacts or Photos, except at the explicit initiative of that user on an individualized basis; do not include a Select All option or default the selection of all contacts. You must provide the user with a clear description of how the message will appear to the recipient before sending it (e.g. What will the message say? Who will appear to be the sender?).

(vi) Data gathered from the HomeKit API, HealthKit, Consumer Health Records API, MovementDisorder APIs, ClassKit or from depth and/or facial mapping tools (e.g. ARKit, Camera APIs, or Photo APIs) may not be used for marketing, advertising or use-based data mining, including by third parties. Learn more about best practices for implementing CallKit, HealthKit, ClassKit, and ARKit.

(vii) Apps using Apple Pay may only share user data acquired via Apple Pay with third parties to facilitate or improve delivery of goods and services.

5.1.3 Health and Health Research

Health, fitness, and medical data are especially sensitive and apps in this space have some additional rules to make sure customer privacy is protected:

(i) Apps may not use or disclose to third parties data gathered in the health, fitness, and medical research context—including from the Clinical Health Records API, HealthKit API, Motion and Fitness, MovementDisorderAPIs, or health-related human subject research—for advertising, marketing, or other use-based data mining purposes other than improving health management, or for the purpose of health research, and then only with permission. Apps may, however, use a user's health or fitness data to provide a benefit directly to that user (such as a reduced insurance premium), provided that the app is submitted by the entity providing the benefit, and the data is not be shared with a third party. You must disclose the specific health data that you are collecting from the device.

(ii) Apps must not write false or inaccurate data into HealthKit or any other medical research or health management apps, and may not store personal health information in iCloud.

(iii) Apps conducting health-related human subject research must obtain consent from participants or, in the case of minors, their parent or guardian. Such consent must include the (a) nature, purpose, and duration of the research; (b) procedures, risks, and benefits to the participant; (c) information about confidentiality and handling of data (including any sharing with third parties); (d) a point of contact for participant questions; and (e) the withdrawal process.

(iv) Apps conducting health-related human subject research must secure approval from an independent ethics review board. Proof of such approval must be provided upon request.

5.1.4 Kids

For many reasons, it is critical to use care when dealing with personal data from kids, and we encourage you to carefully review all the requirements for complying with laws like the Children's Online Privacy Protection Act ("COPPA"), the European Union's General Data Protection Regulation ("GDPR"), and any other applicable regulations or laws.

Apps may ask for birthdate and parental contact information only for the purpose of complying with these statutes, but must include some useful functionality or entertainment value regardless of a person's age.

Apps intended primarily for kids should not include third-party analytics or third-party advertising. This provides a safer experience for kids. In limited cases, third-party analytics and third-party advertising may be permitted provided that the services adhere to the same terms set forth in Guideline 1.3.

Moreover, apps in the Kids Category or those that collect, transmit, or have the capability to share personal information (e.g. name, address, email, location, photos, videos, drawings, the ability to chat, other personal data, or persistent identifiers used in combination with any of the above) from a minor must include a privacy policy and must comply with all applicable children's privacy statutes. For the sake of clarity, the parental gate requirement for the Kid's Category is generally not the same as securing parental consent to collect personal data under these privacy statutes.

As a reminder, Guideline 2.3.8 requires that use of terms like "For Kids" and "For Children" in app metadata is reserved for the Kids Category. Apps not in the Kids Category cannot include any terms in app name, subtitle, icon, screenshots or description that imply the main audience for the app is children.

5.1.5 Location Services
Use Location services in your app only when it is directly relevant to the features and services provided by the app. Location-based APIs shouldn't be used to provide emergency services or autonomous control over vehicles, aircraft, and other devices, except for small devices such as lightweight drones and toys, or remote control car alarm systems, etc. Ensure that you notify and obtain consent before collecting, transmitting, or using location data. If your app uses location services, be sure to explain the purpose in your app; refer to the Human Interface Guidelines for best practices on doing so.

5.2 Intellectual Property
Make sure your app only includes content that you created or that you have a license to use. Your app may be removed if you've stepped over the line and used content without permission. Of course, this also means someone else's app may be removed if they've "borrowed" from your work. If you believe your intellectual property has been infringed by another developer on the App Store, submit a claim via our web form. Laws differ in different countries, but at the very least, make sure to avoid the following common errors:

5.2.1 Generally: Don't use protected third-party material such as trademarks, copyrighted works, or patented ideas in your app without permission, and don't include misleading, false, or copycat representations, names, or metadata in your app bundle or developer name. Apps should be submitted by the person or legal entity that owns or has licensed the intellectual property and other relevant rights.

5.2.2 Third-Party Sites/Services: If your app uses, accesses, monetizes access to, or displays content from a third-party service, ensure that you are specifically permitted to do so under the service's terms of use. Authorization must be provided upon request.

5.2.3 Audio/Video Downloading: Apps should not facilitate illegal file sharing or include the ability to save, convert, or download media from third-party sources (e.g. Apple Music, YouTube, SoundCloud, Vimeo, etc.) without explicit authorization from those sources.

Streaming of audio/video content may also violate Terms of Use, so be sure to check before your app accesses those services. Documentation must be provided upon request.

5.2.4 Apple Endorsements: Don't suggest or imply that Apple is a source or supplier of the App, or that Apple endorses any particular representation regarding quality or functionality. If your app is selected as an "Editor's Choice," Apple will apply the badge automatically.

5.2.5 Apple Products: Don't create an app that appears confusingly similar to an existing Apple product, interface (e.g. Finder), app (such as the App Store, iTunes Store, or Messages) or advertising theme. Apps and extensions, including third-party keyboards and Sticker packs, may not include Apple emoji. iTunes music previews may not be used for their entertainment value (e.g. as the background music to a photo collage or the soundtrack to a game) or in any other unauthorized manner. If your app displays Activity rings, they should not visualize Move, Exercise, or Stand data in a way that resembles the Activity control. The Human Interface Guidelines have more information on how to use Activity rings.

5.3 Gaming, Gambling, and Lotteries

Gambling, gaming, and lotteries can be tricky to manage and tend to be one of the most regulated offerings on the App Store. Only include this functionality if you've fully vetted your legal obligations everywhere you make your app available and are prepared for extra time during the review process. Some things to keep in mind:

5.3.1 Sweepstakes and contests must be sponsored by the developer of the app.

5.3.2 Official rules for sweepstakes, contests, and raffles must be presented in the app and make clear that Apple is not a sponsor or involved in the activity in any manner.

5.3.3 Apps may not use in-app purchase to purchase credit or currency for use in conjunction with real money gaming of any kind, and may not enable people to purchase lottery or raffle tickets or initiate fund transfers in the app.

5.3.4 Apps that offer real money gaming (e.g. sports betting, poker, casino games, horse racing) or lotteries must have necessary licensing and permissions in the locations where the App is used, must be geo-restricted to those locations, and must be free on the App Store. Illegal gambling aids, including card counters, are not permitted on the App Store. Lottery apps must have consideration, chance, and a prize.

5.4 VPN Apps

Apps offering VPN services must utilize the NEVPNManager API and may only be offered by developers enrolled as an organization. You must make a clear declaration of what user data will be collected and how it will be used on an app screen prior to any user action to purchase or otherwise use the service. Apps offering VPN services may not sell, use, or disclose to third parties any data for any purpose, and must commit to this in their privacy policy. VPN apps must not violate local laws, and if you choose to make your VPN app available in a territory that requires a VPN license, you must provide your license information in the App Review Notes field. Parental control, content blocking, and security apps, among others, from approved providers may also use the NEVPNManager API. Apps that do not comply with this guideline will be removed from the App Store and you may be removed from the Apple Developer Program.

5.5 Mobile Device Management

Mobile Device Management Apps that offer Mobile Device Management (MDM) services must request this capability from Apple. Such apps may only be offered by commercial enterprises (such as business organizations, educational institutions, or government agencies), and in limited cases, companies using MDM for parental control services or device security. You must make a clear declaration of what user data will be collected and how it will be used on an app screen prior to any user action to purchase or otherwise use the service.

MDM apps must not violate any applicable laws. Apps offering MDM services may not sell, use, or disclose to third parties any data for any purpose, and must commit to this in their privacy policy. In limited cases, third-party analytics may be permitted provided that the services only collect or transmit data about the performance of the developer's MDM app, and not any data about the user, the user's device, or other apps used on that device. Apps offering configuration profiles must also adhere to these requirements. Apps that do not comply with this guideline will be removed from the App Store and you may be removed from the Apple Developer Program.

5.6 Developer Code of Conduct
Please treat everyone with respect, whether in your responses to App Store reviews, customer support requests, or when communicating with Apple, including your responses in Resolution Center. Do not engage in harassment of any kind, discriminatory practices, intimidation, bullying, and don't encourage others to engage in any of the above.

Customer trust is the cornerstone of the App Store's success. Apps should never prey on users or attempt to rip-off customers, trick them into making unwanted purchases, force them to share unnecessary data, raise prices in a tricky manner, charge for features or content that are not delivered, or engage in any other manipulative practices within or outside of the app.

5.6.1 App Store Reviews
App Store customer reviews can be an integral part of the app experience, so you should treat customers with respect when responding to their comments. Keep your responses targeted to the user's comments and do not include personal information, spam, or marketing in your response.

Use the provided API to prompt users to review your app; this functionality allows customers to provide an App Store rating and review without the inconvenience of leaving your app, and we will disallow custom review prompts.

After You Submit

Once you've submitted your app and metadata in App Store Connect and you're in the review process, here are some things to keep in mind:

- **Timing**: App Review will examine your app as soon as we can. However, if your app is complex or presents new issues, it may require greater scrutiny and consideration. And remember that if your app is repeatedly rejected for the same guideline violation or you've attempted to manipulate the App Review process, review of your app will take longer to complete. Learn more about App Review.
- **Status Updates**: The current status of your app will be reflected in App Store Connect, so you can keep an eye on things from there.
- **Expedite Requests**: If you have a critical timing issue, you can request an expedited review. Please respect your fellow developers by seeking expedited review only when you truly need it. If we find you're abusing this system, we may reject your requests going forward.
- **Release Date**: If your release date is set for the future, the app will not appear on the App Store until that date, even if it is approved by App Review. And remember that it can take up to 24-hours for your app to appear on all selected storefronts.

- **Rejections**: Our goal is to apply these guidelines fairly and consistently, but nobody's perfect. If your app has been rejected and you have questions or would like to provide additional information, please use the Resolution Center to communicate directly with the App Review team. This may help get your app on the store, and it can help us improve the App Review process or identify a need for clarity in our policies. If you still disagree with the outcome, please submit an appeal.

We're excited to see what you come up with next!

Last Updated: 04 March 2020

Copyright © 2020 Apple Inc. All rights reserved.

CIVIL COVER SHEET

The JS-CAND 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS
Epic Games, Inc.

(b) County of Residence of First Listed Plaintiff
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
See attachment.

DEFENDANTS
Apple, Inc.

County of Residence of First Listed Defendant Santa Clara
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☐ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment Of Veteran's Benefits
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☐ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury -Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury – Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities–Employment
- ☐ 446 Amer. w/Disabilities–Other
- ☐ 448 Education

PRISONER PETITIONS

HABEAS CORPUS
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

OTHER
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee–Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC § 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC § 158
- ☐ 423 Withdrawal 28 USC § 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent–Abbreviated New Drug Application
- ☐ 840 Trademark

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS–Third Party 26 USC § 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC § 3729(a))
- ☐ 400 State Reapportionment
- ☒ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced & Corrupt Organizations
- ☐ 480 Consumer Credit
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

- ☒ 1 Original Proceeding
- ☐ 2 Removed from State Court
- ☐ 3 Remanded from Appellate Court
- ☐ 4 Reinstated or Reopened
- ☐ 5 Transferred from Another District *(specify)*
- ☐ 6 Multidistrict Litigation–Transfer
- ☐ 8 Multidistrict Litigation–Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
15 U.S.C. § 1; 15 U.S.C. § 2; 15 U.S.C. § 26

Brief description of cause:
Cause for injunctive relief to address violations of Sections 1 and 2 of the Sherman Act and other laws.

VII. REQUESTED IN COMPLAINT:

☐ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, Fed. R. Civ. P.

DEMAND $

CHECK YES only if demanded in complaint:
JURY DEMAND: ☐ Yes ☒ No

VIII. RELATED CASE(S), IF ANY *(See instructions):*

JUDGE Yvonne Gonzalez Rogers DOCKET NUMBER 4:19cv03074

IX. DIVISIONAL ASSIGNMENT (Civil Local Rule 3-2)

(Place an "X" in One Box Only) ☐ **SAN FRANCISCO/OAKLAND** ☐ **SAN JOSE** ☐ **EUREKA-MCKINLEYVILLE**

DATE 08/13/2020 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Paul Riehle

Attachment to Civil Cover Sheet

I. PLAINTIFF'S ATTORNEYS

FAEGRE DRINKER BIDDLE & REATH LLP
Paul J. Riehle
Four Embarcadero Center
San Francisco, California 94111
Telephone: (415) 591-7500

CRAVATH, SWAINE & MOORE LLP
Christine A. Varney*
Katherine B. Forrest*
Gary A. Bornstein*
Yonatan Even*
M. Brent Byars*
Worldwide Plaza
825 Eighth Avenue
New York, NY 10019
Phone: (212) 474-1000

* *Pro hac vice* application forthcoming

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS-CAND 44

Authority For Civil Cover Sheet. The JS-CAND 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved in its original form by the Judicial Conference of the United States in September 1974, is required for the Clerk of Court to initiate the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)."

II. Jurisdiction. The basis of jurisdiction is set forth under Federal Rule of Civil Procedure 8(a), which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

(1) United States plaintiff. Jurisdiction based on 28 USC §§ 1345 and 1348. Suits by agencies and officers of the United States are included here.

(2) United States defendant. When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

(3) Federal question. This refers to suits under 28 USC § 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

(4) Diversity of citizenship. This refers to suits under 28 USC § 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; **NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS-CAND 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerk(s) in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. Origin. Place an "X" in one of the six boxes.

(1) Original Proceedings. Cases originating in the United States district courts.

(2) Removed from State Court. Proceedings initiated in state courts may be removed to the district courts under Title 28 USC § 1441. When the petition for removal is granted, check this box.

(3) Remanded from Appellate Court. Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

(4) Reinstated or Reopened. Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

(5) Transferred from Another District. For cases transferred under Title 28 USC § 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

(6) Multidistrict Litigation Transfer. Check this box when a multidistrict case is transferred into the district under authority of Title 28 USC § 1407. When this box is checked, do not check (5) above.

(8) Multidistrict Litigation Direct File. Check this box when a multidistrict litigation case is filed in the same district as the Master MDL docket.

Please note that there is no Origin Code 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statute.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC § 553. Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Federal Rule of Civil Procedure 23.

Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS-CAND 44 is used to identify related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

IX. Divisional Assignment. If the Nature of Suit is under Property Rights or Prisoner Petitions or the matter is a Securities Class Action, leave this section blank. For all other cases, identify the divisional venue according to Civil Local Rule 3-2: "the county in which a substantial part of the events or omissions which give rise to the claim occurred or in which a substantial part of the property that is the subject of the action is situated."

Date and Attorney Signature. Date and sign the civil cover sheet.