

1 THEODORE J. BOUTROUS JR., SBN 132099

tboutrous@gibsondunn.com

2 RICHARD J. DOREN, SBN 124666

rdoren@gibsondunn.com

3 DANIEL G. SWANSON, SBN 116556

dswanson@gibsondunn.com

4 JAY P. SRINIVASAN, SBN 181471

jsrinivasan@gibsondunn.com

5 JASON C. LO, SBN 219030

jlo@gibsondunn.com

6 GIBSON, DUNN & CRUTCHER LLP

333 South Grand Avenue Los Angeles, CA 90071

7 Telephone: 213.229.7000

Facsimile: 213.229.7520

8 VERONICA S. MOYÉ (Texas Bar No.

9 24000092; pro hac vice)

vmoye@gibsondunn.com

10 GIBSON, DUNN & CRUTCHER LLP

2100 McKinney Avenue, Suite 1100

11 Dallas, TX 75201

Telephone: 214.698.3100

12 Facsimile: 214.571.2900

MARK A. PERRY, SBN 212532

mperry@gibsondunn.com

CYNTHIA E. RICHMAN (D.C. Bar No.
492089; pro hac vice)

crichman@gibsondunn.com

GIBSON, DUNN & CRUTCHER LLP

1050 Connecticut Avenue, N.W.

Washington, DC 20036

Telephone: 202.955.8500

Facsimile: 202.467.0539

ETHAN D. DETTMER, SBN 196046

edettmer@gibsondunn.com

GIBSON, DUNN & CRUTCHER LLP

555 Mission Street

San Francisco, CA 94105

Telephone: 415.393.8200

Facsimile: 415.393.8306

Attorneys for Defendant APPLE INC.

13
14 UNITED STATES DISTRICT COURT

15 FOR THE NORTHERN DISTRICT OF CALIFORNIA

16 OAKLAND DIVISION

17
18 EPIC GAMES, INC.

19 Plaintiff,

20 v.

21 APPLE INC.,

22 Defendant.

Case No. 20-cv-05640-YGR

**DECLARATION OF
TRYSTAN KOSMYNKA**

The Honorable Yvonne Gonzalez Rogers

1 I, Trystan Kosmyнка, declare as follows:

2 1. I am employed as Senior Director of App Review at Apple Inc. (“Apple”). In my role
3 as Senior Director of App Review, I run the team and organization that reviews apps submitted for
4 distribution through Apple’s App Store. I am also a member of the Executive Review Board, which
5 creates policies that apply to Apple’s App Store and app review process. I have personal knowledge
6 of the matters stated herein and, if called upon to do so, I could and would testify competently hereto.

7 **Apple’s App Review Guidelines and Review Process**

8 2. Apple is committed to keeping the App Store a safe and trusted place for users to get
9 apps and a great opportunity for all developers to be successful. As part of that commitment, Apple
10 promulgates App Review Guidelines and reviews every app and app update submitted for distribution
11 through the App Store using a rigorous and sophisticated review process. Apple performs
12 computerized static and dynamic analysis, as well as manual human review, on the compiled software,
13 or “binary” file, that a developer submits for App Review, along with metadata including screenshots,
14 images, pricing information, and text describing the app. And if an app contains in-app purchases using
15 Apple’s In-App Purchase (“IAP”), which is part of Apple’s integrated commerce engine, the App
16 Review team reviews every one of those offerings to confirm whether they deliver the good or service
17 that the user pays for and expects. We investigate whether each transaction will actually result in the
18 delivery of the expected content, whether the purchased content is consistent with the overall app, and
19 whether the transaction may have other characteristics that could mark it as a scam or mislead users.

20 3. Apple’s App Review Guidelines are intended to protect users against apps that are
21 malicious, dangerous, offensive, scams, invade user privacy, or contain malware, among other threats
22 that would harm them. We have five pillars of the App Review Guidelines—Safety, Performance,
23 Business Model, Design, and Legal—all of which are evaluated by Apple when reviewing apps. From
24 our perspective, these pillars are key to users knowing what they are getting when they download an
25 app, and how that app will treat their data, before they make the decision to download.

26 4. The Business pillar requires the business model of an app—the way that a developer
27 tries to monetize an app—to be clear. The Guidelines make clear that Apple will not distribute apps
28 and digital products or services that are clear rip-offs. They set out a universal set of rules that require

1 apps selling subscriptions to contain clear and conspicuous pricing and clearly describe what the user
2 will get for that pricing. The Guidelines also are intended to ensure that apps perform the way they are
3 described as performing and protect users against scams. For example, Apple prohibits apps that hold
4 users hostage by refusing to provide paid-for functionality until the user consents to unnecessary data
5 access. Apple also requires that apps offering “loot boxes,” or mechanisms that provide randomized
6 virtual items for purchase, must disclose the odds of receiving each type of item to customers prior to
7 purchase. Nor can credits or in-game currencies purchased via in-app purchase expire under the
8 Guidelines.

9 5. Apple’s App Review Guidelines also seek to protect against invasions of user privacy,
10 by prohibiting apps that attempt to manipulate, trick, or force people to consent to unnecessary data
11 access, or that seek to access data not necessary to accomplish the relevant tasks of the app. The App
12 Store is designed to help users better understand an app’s privacy practices even before they make the
13 decision to download that app onto their device. Every developer is required to submit app privacy
14 labels (which we also refer to colloquially as “nutrition labels”) with every app and app update
15 submitted to the App Store. App privacy labels are intended to inform users what data will be collected
16 from the app and how it will be used.

17 6. Apple holds all apps available in the App Store to a high standard for privacy, security,
18 and content. App Review has detected and prevented acts of fraud, attempted theft, and other ill-
19 intentioned conduct. Apple receives approximately one hundred thousand submissions of apps and
20 app reviews per week, with a yearly total of over 4 million submissions. In 2019, for example, Apple
21 received 4,808,685 submissions. Of those submissions, 1,747,278 were rejected because they did not
22 meet the standards for privacy, security, reliability, performance, and quality set out in Apple’s App
23 Review Guidelines. This amounted to a rejection rate of 36 percent in 2019, which is roughly consistent
24 with the rejection rates for 2017 and 2018. In 2020, the rejection rate rose to around 40 percent.

25 7. In 2020 alone, Apple rejected more than 48,000 apps because they contained hidden or
26 undocumented features, more than 150,000 apps because they were found to be spam, copycats, or
27 misleading to users in ways such as manipulating them into making a purchase, and more than 215,000
28 apps because they contained violations of Apple’s user privacy-protecting Guidelines. Apple also

1 terminated 470,000 developer accounts and rejected an additional 205,000 developer enrollments over
2 fraud concerns, to prevent them from submitting bad apps to the App Store. These efforts complement
3 sophisticated fraud detection techniques that Apple performs on purchases made using Apple’s secure
4 commerce engine on the App Store. Apple has been able to identify the use of stolen cards during
5 purchasing and other potentially fraudulent transactions. Apple has published statistics regarding these
6 efforts in the Press Release attached as Exhibit A. Though these efforts, we have built critical trust
7 with users and as a result Apple’s brand is synonymous with security, privacy, and reliability.

8 **Guideline 3.1.1 and the Court’s Injunction**

9 8. Among Apple’s App Review Guidelines is Guideline 3.1.1., which says in its first
10 paragraph: “If you want to unlock features or functionality within your app, (by way of example:
11 subscriptions, in-game currencies, game levels, access to premium content, or unlocking a full version),
12 you must use in-app purchase. Apps may not use their own mechanisms to unlock content or
13 functionality, such as license keys, augmented reality markers, QR codes, etc. Apps and their metadata
14 may not include buttons, external links, or other calls to action that direct customers to purchasing
15 mechanisms other than in-app purchase.” I understand that, on September 10, 2021, the Court issued
16 an injunction against Apple relating to this Guideline.

17 9. Since September 10, 2021, Apple has received multiple questions from developers
18 about this injunction and what it means. Developers, including those with previous rejections under
19 Guideline 3.1.1, have been resubmitting or replying to the App Review team to ask how the guidelines
20 are changing or whether they need to continue to comply with Guideline 3.1.1. Their communications,
21 some of which point to news articles, show substantial confusion about the injunction’s terms. Many
22 of these developers appear to believe that the injunction prohibits Apple from requiring the use of IAP
23 generally, and instead permits developers to utilize payment mechanisms other than IAP inside their
24 apps. One developer wrote: “I would like to know how (and when) the guidelines are changing in
25 relation to the ruling that Apple must now allow other forms of in-app purchases for apps uploaded to
26 the App Store.” Another developer wrote: “now that the new US court ruling allowed developers to
27 have 3rd party payment systems, can we now publish an app that charges money from the users, without
28 adding apple-payment solutions at the beginning?” Still another developer wrote: “Are you suggesting

1 that we still need to implement in-app purchase to get our app approved and it's a compulsory
2 requirement?"

3 10. Along with others at Apple, I am currently studying the effect of the change to Guideline
4 3.1.1 in light of the Court's ruling. At a high level, it is my judgment that, without thoughtful
5 restrictions in place to protect consumers, developers, and the iOS platform, this change will harm
6 users, developers, and the iOS platform more generally.

7 11. Guideline 3.1.1 currently allows Apple to ensure that users who purchase digital goods
8 or services in an app receive what they paid for, on the actual terms that they were informed of and
9 agreed to, and that the payment will occur in a secure manner, protected against fraud and theft of their
10 personal information. The combination of Guideline 3.1.1 and IAP equalizes the playing field for every
11 user and every developer, so that every user knows that any IAP purchase from any developer's app
12 available in the App Store will occur in a safe and verified manner. Guideline 3.1.1 thus has formed
13 one of the backbones of the App Store's protections and been critical to Apple's ability to offer a
14 curated app store environment.

15 12. Apple's IAP offers a secure payment system that protects user payment information and
16 details. It reflects the clear and straightforward disclosure of the price that will be charged for a digital
17 good or service at time of purchase or through subscriptions, as well as notifications when a free trial
18 is about to end and a user is about to be charged. Apple provides many additional services and benefits
19 to customers, many of which are unique to Apple's commerce engine. IAP records sales and creates
20 receipts for those purchases, so purchases can be verified. It enables the completion or restoration of
21 purchases, whether in situations where a user hit the "buy" button for an IAP purchase and the
22 developer did not deliver the content for some technical reason or in situations where a user wants to
23 put an app and in-app-purchased content on a new device. It allows Apple, developers, and users to
24 verify whether a receipt for an IAP purchase is authentic and allows Apple to respond to the hundreds
25 of thousands of reports that we receive every day from users who need help with a developer that has
26 failed to deliver a promised digital good. It facilitates family sharing so that app purchases and services
27 can be shared across family members. It protects users against unintended or fraudulent purchases with
28 a "content check" feature to make sure a user has not made a duplicative purchase, and an "ask to buy"

1 feature that allows parents to approve or block a child’s in-app purchase. Plus, IAP transactions are
2 monitored by Apple’s anti-fraud technology, to detect and protect against the use of stolen cards in IAP
3 purchases of digital goods and services (including for the purpose of laundering or other illicit
4 purposes).

5 13. Users who make a payment for digital content thus expect that they are providing their
6 personal and financial information in a secure manner, in exchange for that verified purchase. When
7 users make purchases of digital content in the App Store using IAP, Apple is uniquely positioned to
8 verify the delivery of the content and to provide customer support for the transaction. Conversely,
9 Guideline 3.1.1 does not apply to transactions involving delivery of physical goods and services, in
10 part because Apple has no ability to verify delivery and troubleshoot problems with such purchases.

11 14. Purchases of digital content and services are also vulnerable to fraudulent manipulation.
12 We have observed social engineering attacks attempted through digital content purchases. The App
13 Review team reviews IAP purchases to screen for such attempts, along with subscription pricing
14 information contained in an app. The App Review team has taken action on many apps that try to
15 defraud or maliciously change pricing information in apps after review. In fact, the specific restrictions
16 in Guideline 3.1.1 have arisen in response to threats detected in apps. With respect to social engineering
17 attacks, some apps have tried to change their subscription pricing after review to make their pricing
18 information opaque or otherwise mislead the user. For example, some developers have stated that the
19 subscription will charge \$1 per day for a year, rather than \$365 per year, in order to conceal the
20 complete cost. Other apps have tried to offer a range of prices for IAP (such as 1 virtual crop, 10 virtual
21 crops, 100 virtual crops, 1000 virtual crops) where one of the prices (often in the middle) is
22 disproportionately higher than the other, with the goal of conditioning the user to quickly pay that
23 disproportionately high price. Still other apps place flashing arrows around the “okay” button or the
24 “allow” button as a way to condition the user to providing a quick permission, or flash a series of pop-
25 up screens requiring a “yes” answer immediately before popping up an IAP purchase screen. Other
26 developers have tried to abuse Apple’s Touch ID functionality by first requiring Touch ID to log into
27 an app, and then immediately surfacing a purchase screen while Touch ID is still operative—and with
28 pricing that is exorbitantly disproportionate to the content to be purchased. And these examples of

1 malicious apps are not the only time that we have seen developers try to take advantage of user
2 confidence in the safety, security, and reliability of apps offered on the App Store in order to mislead
3 or defraud users. By the same token, there is a risk that bad actors will seek to exploit user expectation
4 that payment mechanisms to which an app directs users (and particularly payment links embedded in
5 an app) would be safe places where users can securely provide their payment, email address, and other
6 personal and contact information.

7 15. To my knowledge, Apple has never permitted external payment links or other payment
8 mechanisms for the purchase of digital goods and services within an app. External payment
9 mechanisms that operate outside of Apple's secure commerce engine not benefit from Apple's IAP or
10 App Review protections and benefits. When users utilize external payment links, they are thus no
11 longer utilizing a payment mechanism that Apple secures, verifies, and protects from fraud. Apple
12 does not have visibility into the payment transactions and cannot verify that the users actually paid for
13 the good with a valid payment mechanism or received the product or feature that they paid for. Nor
14 can Apple review the purchase offerings for compliance with the App Review Guidelines or conduct
15 anti-fraud monitoring on purchases and payments made on an external website. Apple cannot make
16 sure that there is a clear way to cancel subsequent charges to the payment information entered on an
17 external website. And Apple cannot ensure that an external website protects a user's privacy or
18 payment information, or that it conforms to the app's privacy nutrition labels that the developer
19 submitted to Apple during the App Review process. And even if Apple could check these websites
20 during the review process, Apple cannot prevent developers from, after approval of their app or app
21 update, altering an external website. Not only does this introduce security and privacy risks, but it also
22 means Apple is unable to respond to and provide refunds for users who need help with a developer that
23 has failed to deliver on a promised digital good, as well as the ability to identify and take action to stop
24 fraudulent developers.

25 16. Steering consumers to external payment mechanisms thus will expose users with much
26 greater frequency to the risks of external payment links and, consequently, lower user confidence in
27 the safety, security, and reliability of digital content purchases and mechanisms. Developers will suffer
28 from this lowered confidence as well, as users will be less inclined to make purchases. More generally,

1 steering consumers to external payment mechanisms will affect the promise of a curated app store
2 where users know that, when they want to buy a digital good or service in an app, they will actually
3 receive what they paid for and that the payment will occur in a secure manner, protected against fraud
4 and theft of their personal information.

5 17. In view of these risks, Apple is actively investigating mechanisms for safeguarding
6 users, developers, the App Store, and the iOS platform to the extent possible. Apple’s App Store and
7 IAP functionality are deeply integrated into the iOS ecosystem and rely upon and utilize iOS device
8 hardware and software. Apple has continued to work on the development and improvement of IAP
9 into the iOS ecosystem since its roll-out, with a series of systemic changes that each have required
10 significant consideration and time. In fact, Apple just released StoreKit 2, an improved version of the
11 StoreKit API that enables IAP functionality, after extensive work and time. StoreKit 2 improves the
12 security of purchases, from the way that developers can resolve purchase issues, to the way that users
13 can request refunds and manage their individual app subscriptions.

14 18. If users can be steered to external payment mechanisms, we will have to consider the
15 impact on the layers of protection that IAP offers: protections such as “Ask to Buy” feature and parental
16 controls for apps for children, the way in which Face ID or Touch ID can be used to authorize a
17 purchase in all apps, and the way that purchases can be completed and restored on a user’s devices,
18 among others. It will require substantial engineering and other changes to the App Store, to App
19 Review and its tools, and to all of platforms and devices that interact with and rely upon the App Store.
20 Indeed, we have previously had to make engineering changes to the operating system along with
21 Guideline changes in response to risks that have been detected in apps. In addition, we have to consider
22 customer service features such as the current refund and dispute resolution mechanisms for addressing
23 complaints by users and developers about failed delivery content and fraudulent purchases. Plus we
24 have to evaluate whether potential new Guidelines and other protective features have to be developed
25 for the App Store. All of this is in addition to the development of new App Review processes and
26 computer tools to account for the new risks. Ultimately, these questions require consideration of the
27 very security concerns that Apple has combatted with the use of IAP and the way in which users interact
28

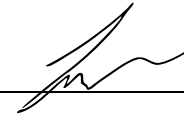
1 with their devices—all of which will impact the trust and confidence that users currently hold in the
2 App Store.

3 * * *

4 I declare under penalty of perjury under the laws of the United States of America that the
5 foregoing is true and correct.

6 Executed on October 8, 2021 at San Jose, California.

7
8 By: _____



9 Trystan Kosmyнка
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28