BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
LESLIE E. HURST (178432)
THOMAS J. O'REARDON II (247952)
ADAM M. BUCCI (327312)
501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
lhurst@bholaw.com
toreardon@bholaw.com
abucci@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW (*pro hac vice forthcoming*)
ANTHONY L. PARKHILL (*pro hac vice forthcoming*)
205 W. Randolph Street, #1630
Chicago, IL 60606
Tel: 312/621/2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiff

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA – SAN JOSE DIVISION

DANYELL SHIN, on behalf of herself and all others similarly situated, Plaintiff, v. APPLE, INC., Defendant.	Case No. 5:25-cv-5000 **CLASS ACTION COMPLAINT** **CLASS ACTION** **JURY TRIAL DEMANDED**

Plaintiff Danyell Shin, on behalf of herself and all others similarly situated, hereby files her complaint against Apple, Inc. ("Apple" or "Defendant"), and in support thereof states:

INTRODUCTION

1. Apple authorized and maintained malicious applications in its "App Store" that allowed the theft of personal financial assets while representing that apps in its App Store had been vetted and reviewed by Apple and were safe and secure.

2. Apple has built a business model that depends not only on selling hardware such as iPhones and iPads, but also on providing consumers with a curated selection of applications through the App Store. By maintaining exclusive control over the applications that may be downloaded on Apple devices, Apple has structured its ecosystem so that customers rely on Apple for the perceived safety and reliability of the App Store. Apple has actively and extensively represented to consumers that apps on the App Store are thoroughly vetted, trustworthy, and secure. Apple has actively represented that its App Store apps which are used for cryptocurrency trading come from approved financial institutions and comply with all applicable laws.

3. These representations foster consumer trust, which, in turn, incentivizes consumers to purchase Apple devices over competing brands. Apple's campaign to promote the safety and trustworthiness of its App Store directly contributes to increased sales of iPhones and other Apple products, as consumers reasonably believe that Apple's devices provide a safer and more secure user experience. Without this assurance of security, fewer consumers would be inclined to purchase Apple devices, as they might perceive other smartphones or tablets as equally secure or better suited to meet their needs.

4. Apple's assertions regarding the safety and legitimacy of App Store apps thus serve a dual purpose: enhancing the appeal of Apple's ecosystem while driving hardware sales. This is not merely a platform for app distribution but a cornerstone of Apple's competitive advantage in the smartphone and tablet market. Consequently, Apple profits not only from app sales or in-app purchases but also from free apps because Apple profits significantly from the added value that this perceived security brings to its devices, making the continued representation of app safety integral to Apple's market strategy and business growth.

5. Plaintiff and Class members relied on Apple's express representations and ongoing and long-standing campaign of representing that its App Store is "a safe and trusted place" when they downloaded applications purporting to be digital asset trading applications. Unknown to Plaintiff and Class members, these applications, including the Swiftcrypt app Plaintiff downloaded, were "spoofing" programs created for the sole purpose of stealing fiat and cryptocurrency by obtaining consumers' account information and thereafter routing Class members' assets to the perpetrators' personal accounts. Not knowing this, and relying on Apple's express and longstanding representations that apps from its App Store had been vetted and were safe and legally compliant, Plaintiff and Class members downloaded the app from the Apple App Store. Subsequently, after following instructions contained in the apps to deposit funds, and after what appeared to be legitimate trades and growth of their funds, their accounts were frozen and all the money they invested was stolen in a cryptocurrency investment scam known as "pig butchering."[1]

6. Apple's affirmative representations and the general impression that it has cultivated that apps from its App Store could be trusted and were safe and secure because of Apple's rigorous vetting and review process were false and misleading. As a result of Apple's misrepresentations, and its failure to take appropriate corrective or remedial action, Apple has caused Plaintiff and Class members to download an app created solely for "pig butchering" schemes and hence to suffer significant economic losses. Defendant's conduct is in violation of California's Consumers Legal Remedies Act ("CLRA"), Civil Code § 1750, *et seq*. and California's Unfair Competition Law ("UCL"), Business and Professions Code § 17200, *et seq*.

7. By virtue of this class action, Plaintiff seeks to enjoin Apple's unlawful practices and to require that Apple to compensate Plaintiff and members of the Class for the losses they have incurred because of its misconduct.

[1] "Pig butchering" is "named in reference to the practice of fattening a pig before slaughter. It is a type of confidence and investment fraud in which the victim is gradually lured into making increasing monetary contributions, generally in the form of cryptocurrency, to a seemingly sound investment before the scammer disappears with the contributed monies." *See* Office of Inspector General, *Pig Butchering Scams*, FDICOIG, https://www.fdicoig.gov/pig-butchering-scams (last accessed May 28, 2025).

PARTIES

8. Plaintiff Danyell Shin is an individual, over 18 years of age, and a citizen of the State of Illinois, the County of Cook.

9. Defendant Apple, Inc. is a California corporation with its principal place of business at One Apple Park Way, Cupertino, California 95014.

JURISDICTION AND VENUE

10. Jurisdiction is proper under the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(d), because, on information and belief, the proposed Class consists of 100 or more members; many of the members are citizens of states that are diverse from the state of Defendant's citizenship; and the amount in controversy exceeds $5,000,000, exclusive of costs and interest.

11. This Court may exercise personal jurisdiction over Apple, who has availed itself of the jurisdiction of this Court through acts and omissions, including but not limited to, having its principal place of business in this District, advertising its services in this District, selling products and services to consumers in this District, and by otherwise conducting business in this District; furthermore, various agreements between Apple and the Class select the Courts of this State as the proper forum for all disputes.

12. Venue is therefore proper in this forum pursuant to 28 U.S.C. § 1391(b), and further, as Apple is located in this judicial district and/or a substantial part of the acts or omissions giving rise to the claims herein occurred in the same.

INTRADISTRICT ASSIGNMENT

13. Pursuant to Civil L.R. 3-2(c) and (e), assignment to the San Jose Division is proper because a substantial part of the conduct which gives rise to Plaintiff's claims occurred in Santa Clara County, where Apple resides.

GENERAL ALLEGATIONS

Apple and the App Store

14. Apple is one of the largest mobile and tablet application providers in the world, through its universally known "App Store."

15. Apple describes the App Store to consumers as follows: [2]

The apps you love.
From a place you can trust.

For over a decade, the App Store has proved to be a safe and trusted place to discover and download apps. But the App Store is more than just a storefront — it's an innovative destination focused on bringing you amazing experiences. And a big part of those experiences is ensuring that the apps we offer are held to the highest standards for privacy, security, and content. Because we offer nearly two million apps — and we want you to feel good about using every single one of them.

16. Apple has worked for decades to build and promote a reputation of providing apps that are safe and can be trusted. Over time, Apple has established an image that its App Store is carefully curated, with each app undergoing a rigorous review to ensure it meets Apple's security standards. This long-standing marketing message has fostered an inherent belief among consumers that apps on the App Store are safe by default.

17. Apple has distinguished itself in the tech industry as a company committed to user privacy and security. Consumers have come to associate Apple products with high standards of protection, further encouraging the reasonable belief that any app available on the App Store is secure and free from fraudulent intent. This association reinforces reasonable consumers' belief that Apple's vetting process extends to protecting them from scams.

18. Apple exercises exclusive control over app distribution on iOS devices, disallowing alternative app sources or sideloading. This exclusivity suggests to consumers that Apple is confident in its review and vetting process, leading users to believe that Apple has effectively

[2] *App Store*, Apple, https://www.apple.com/app-store/ (last accessed May 28, 2025).

shielded them from unsafe or fraudulent applications by eliminating external sources of apps. Indeed, Apple warns users that sideloading "would cripple the privacy and security protections that have made iPhone so secure, and expose users to serious security risks,"[3] reinforcing consumers' belief that Apple-approved apps on the App Store are safe and trustworthy.

19. Apple has promoted its App Store's vetting process as a stringent security measure, publicly detailing how apps are reviewed by experts who assess them for malware, privacy concerns, and other security risks. Apple also promotes and represents that its App Store apps which are used for cryptocurrency transmissions or transactions are appropriately licensed and that apps facilitating cryptocurrency ICOs (Initial Coin Offerings) or other futures trading of cryptocurrency come from approved financial institutions and comply with all applicable laws. Given this promotion, a reasonable consumer would assume that apps made available for download are free from fraudulent or malicious intent, especially for highly regulated fields like finance and digital asset trading.

20. Apple has conveyed to consumers that user safety is a core value, underscored by statements such as "Download with confidence" and assurances that the App Store is a "safe and trusted place." Given the prevalence of these messages, consumers are led to believe that Apple's security and vetting practices are specifically designed to prevent fraudulent schemes like pig butchering scams from being present on the platform.

21. In 2007, Steve Jobs stated that Apple's mission in creating what would become the App Store was to create "an advanced system which will offer developers broad access to natively program the iPhone's amazing software platform while at the same time protecting users from malicious programs."[4] Apple reiterated its approach to the App Store in 2010 when it released the first version of its App Store Review Guidelines, in which it stated "[i]f it sounds like we're control

---

[3] *Building a Trusted Ecosystem for Millions of Apps: A Threat Analysis of Sideloading*, Apple (Oct. 2021), https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps_A_Threat_Analysis_of_Sideloading.pdf.

[4] Adam Engst, *Steve Jobs's iPhone SDK Letter*, TidBits (Oct. 17, 2007), https://tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/.

freaks, well, maybe it's because we're so committed to our users and making sure they have a quality experience with our products."[5]

22. In 2021, Apple published a document titled "Building a Trusted Ecosystem for Millions of Apps: The important role of App Store protections" in which it claims:

> Nearly two million apps are available for users to download on the App Store, with thousands of apps added every week. Given the sheer scale of the App Store platform, ensuring iPhone security and safety was of critical importance to us from the start. . . . [W]e created the App Store, a trusted place where users can safely discover and download apps. On the App Store, apps come from known developers who have agreed to follow our guidelines, and are securely distributed to users free from interference from third parties. We review every single app and each app update to evaluate whether they meet our high standards. This process, which we are constantly working to improve, is designed to protect our users by keeping malware, cybercriminals, and scammers out of the App Store.[6]

23. Apple represents that "[s]ince launching the App Store in 2008, Apple has continued to invest in and develop industry-leading technologies designed to provide users with the safest and most secure experience for downloading apps . . . Today, the App Store stands at the forefront of app distribution, setting the standard for security, reliability, and user experience."[7] It also tells consumers that "[a]s digital threats have evolved in scope and complexity over the years, Apple has expanded its antifraud initiatives to address these challenges and help protect its users. Every day, teams across Apple monitor and investigate fraudulent activity on the App Store, and utilize sophisticated tools and technologies to weed out bad actors and help strengthen the App Store ecosystem."[8]

///

///

---

[5] *See* Leander Kahney, *Here's The Full Text of Apple's New App Store Guidelines*, Cult of Mac (Sept. 9, 2010 8:49 AM), https://www.cultofmac.com/news/heres-the-full-text-of-apples-new-app-store-guidelines.

[6] *Building a Trusted Ecosystem for Millions of Apps: The important role of App Store protections*, Apple (June, 2021), https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf.

[7] *App Store stopped over $7 billion in potentially fraudulent transactions in four years*, Apple (May 14, 2024), https://www.apple.com/newsroom/2024/05/app-store-stopped-over-7-billion-usd-in-potentially-fraudulent-transactions/.

[8] *Id.*

24. In 2025, Apple again reiterated "the App Store's continued investment in fostering the most secure experience for users," and that "the App Store is a trusted destination for users to download their favorite apps and discover new ones."[9] Apple represented to consumers that it "employs a comprehensive approach to combating fraud on the App Store, with teams across the company working to detect, investigate, and prevent malicious activity before it can reach users."[10] Apple assures its users it "will continue to build on its commitment to provide users with the safest and most secure experience on the App Store."[11]

25. In a section titled "App security overview" Apple states:

> Apple provides layers of protection to help ensure that apps are free of known malware and haven't been tampered with. Additional protections enforce that access from apps to user data is carefully mediated. These security controls provide a stable, secure platform for apps, enabling thousands of developers to deliver hundreds of thousands of apps for iOS, iPadOS, and macOS—all without impacting system integrity. And users can access these apps on their Apple devices without undue fear of viruses, malware, or unauthorized attacks.[12]

---

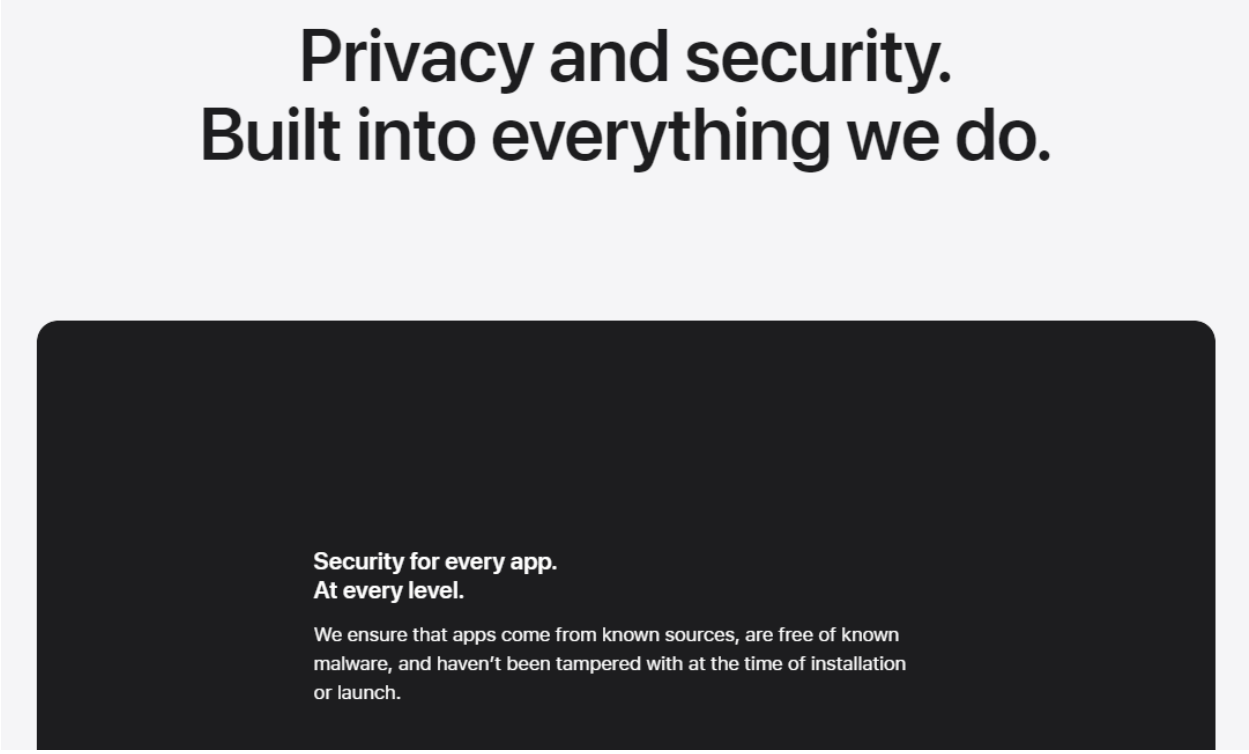
[9] *The App Store prevented more than $9 billion in fraudulent transactions over the last five years*, Apple (May 25, 2025), https://www.apple.com/newsroom/2025/05/the-app-store-prevented-more-than-9-billion-usd-in-fraudulent-transactions/.

[10] *Id.*

[11] *Id.*

[12] *App security overview*, Apple, https://support.apple.com/guide/security/app-security-overview-sec35dd877d0/web (last accessed May 28, 2025).

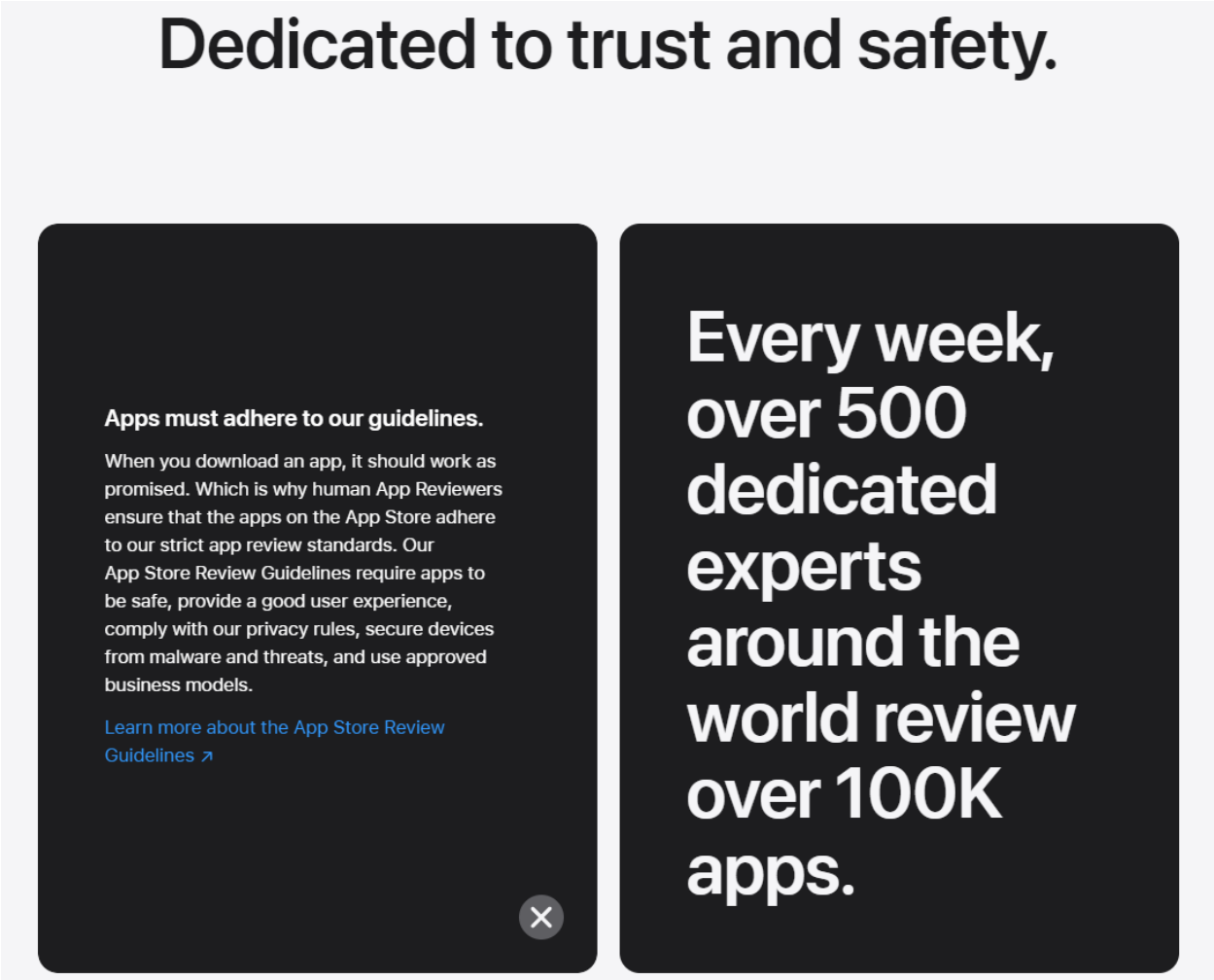
26. Apple on its App Store further represents:[13]



Apple additionally promises it is:[14]

13 *See App Store*, *supra* n.2.

14 *Id.*



27. Apple represents consumers can "**Download with confidence**." It asserts that on its apps, Apple customers can "**Purchase safely and securely.**" And "**Need a refund? AppleCare has your back.**"

28. On its support website, Apple informs users:

> The App Store is a trusted place where users can safely discover and download apps. On the App Store, apps come from identified developers who have agreed to follow Apple guidelines, and are securely distributed to users with cryptographic guarantees against modification. Every single app and each app update is reviewed to evaluate whether it meets requirements for privacy, security and safety. This process, which is being constantly improved, is designed to protect users by keeping malware, cybercriminals and scammers out of the App Store.[15]

[15] *About App Store security*, Apple (Dec. 19, 2024), https://support.apple.com/en-euro/guide/security/secb8f887a15/web.

29. Apple further states, "Unlike other mobile platforms, iOS, iPadOS and visionOS don't allow users to install potentially malicious unsigned apps from websites or to run untrusted apps. Instead . . . all apps must be downloaded from the App Store, where all apps come from identified developers and must pass automated and human review."[16]

30. Apple controls what applications may be sold or provided to consumers through the App Store by a vetting process that involves provision of the proposed application's purpose and a copy of the application itself and any relevant source code, users' guides, and software documentation.[17]

31. As part of Apple's promise that apps from its App Store are vetted for safety and security, it promises that each app on the App Store has met its security standards. The promise that apps on the App Store are rigorously vetted fosters and results in consumer trust of Apple apps. And in Apple's words: "Customer trust is a cornerstone of the App ecosystem. Apps should never prey on users or attempt to rip off customers . . ."[18] According to Apple, "[t]he guiding principle of the App Store is simple—we want to provide a safe experience for users to get apps . . ."[19]

32. According to Apple, it achieves its guiding principle of providing customer safety and establishing a cornerstone of consumer trust in its apps and the App Store, "by offering a highly curated App Store where every app is reviewed by experts . . . We also scan each app for malware and other software that may impact user safety, security, and privacy. These efforts have made Apple's platforms the safest for consumers around the world."[20] Apple also promises "apps that solicit, promote, or encourage criminal or clearly reckless behavior will be rejected."[21]

33. Apple has specific security standards for cryptocurrency exchange apps as follows:[22]

---

16 *Intro to app security for iOS, iPadOS and visionOS*, Apple (Dec. 19, 2024), https://support.apple.com/en-euro/guide/security/secf49cad4db/web.

17 *See, e.g., App Review Guidelines*, Apple Developer, https://developer.apple.com/app-store/review/guidelines (last accessed May 28, 2025).

18 *Id.*

19 *Id.*

20 *Id.*

21 *Id.*

22 *Id.*

3.1.5 Cryptocurrencies:

. . .

(iii) Exchanges: Apps may facilitate transactions or transmissions of cryptocurrency on an approved exchange, provided they are offered only in countries or regions where the app has appropriate licensing and permissions to provide a cryptocurrency exchange.

(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.

34. Defendant represents that as part of its vetting and review process:[23]

Apps that provide services in highly regulated fields (such as banking and financial services, healthcare, gambling, legal cannabis use, 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.

35. Apple also promises immediate correction if issues occur. Apple represents:

In a case where an app makes it into the App Store but is then later discovered to violate guidelines, Apple works with the developer to quickly resolve the issue. In dangerous cases, involving fraud and malicious activity, the app is immediately removed from the App Store and users who downloaded the app can be notified of the app's malicious behavior. [24]

36. Apple makes clear to users that the "goal of App Review is to ensure that apps on the App Store are trustworthy."[25] It also promises "Apple's many layers of security provide users with an unparalleled level of protection from malicious software, giving users peace of mind."[26]

---

23 *Id.*
24 *Supra* n.12.
25 *Supra* n.6.
26 *Id.*

37. Apple's representations of safety and security in the applications offered in the App Store have been made continuously for almost two decades and were a focal point of widespread advertising and marketing representations made by Apple.

38. Apple has successfully cultivated the impression that its products and the apps it vets and makes available in the App Store are safe and trustworthy. Indeed, consumers "are willing to trust apps they download from app stores because of years of positive experiences with the extra scrutiny and safeguards app stores offer. Simply being available on the app stores is now an indicator that an app is reasonably trustworthy for consumers."[27]

39. As described in an article published on February 1, 2023, about illicit pig butchering apps making their way into the Apple App Store, the "presence of the apps in the App Store made the ruse all the more convincing."[28] Researchers from the cybersecurity firm SophosLabs also published an article about pig butchering apps being available in the App Store, stressing that "If criminals can get past these checks [Apple purports to conduct], they have the potential to reach millions of devices. This is what makes it more dangerous for [scam app] victims, as most of those targets are more likely to trust the source if it comes from the official Apple App Store."[29]

40. Apple's business model and sales of iPhones and iPads depends upon the App Store applications being safe and secure for Apple customers.[30]

---

[27] The App Association, *Security and Trust from an App Maker's Point of View*, ACT online (Nov. 2021), https://actonline.org/wp-content/uploads/App-Association-Security-and-Trust-from-an-App-Makers-Point-of-View-November-2021.pdf.

[28] Dan Goodman, *Pig-butchering scam apps sneak into Apple's App Store and Google Play*, arstechnica (Feb. 1, 2023), https://arstechnica.com/information-technology/2023/02/pig-butchering-scam-apps-sneak-into-apples-app-store-and-google-play/ (last accessed May 28, 2025).

[29] Jagadeesh Chandraiah, *Fraudulent 'CryptoRom' trading apps sneak into Apple and Google app store*, Sophos News (Feb. 1, 2023), https://news.sophos.com/en-us/2023/02/01/fraudulent-cryptorom-trading-apps-sneak-into-apple-and-google-app-stores/ (last accessed May 28, 2025).

[30] *See, e.g.*, Michael Gartenberg, *Apple's App store has become an ad-infested imitation of its former self, which is not good for iPhone users or developers*, Bus. Insider (No. 28, 2022 1:48 PM), https://www.businessinsider.com/apples-app-store-has-become-an-ad-plagued-version-of-its-former-self-2022-11 ("Ask just about any Apple executive what makes Apple special and the answer will almost always be Apple's ecosystem — the company's . . . position of creating both the hardware and the software with tight integration.").

41. That is because Apple customers have no other practical or convenient manner in which to download applications for their iPhones or iPads, as Apple maintains rigorous control over applications that can be placed on their devices. If App Store applications are not perceived to be safe, the sales of iPhones and iPads will be negatively impacted.

42. Even when Apple does not directly profit from an application downloaded from the App Store, drawing consumers to its selling forum, as opposed to other fora, has considerable business advantage to Apple, as it encourages consumers to purchase Apple products and dissuades consumers from purchasing other devices. The App Store's perception of trust and safety has "been central to the growth in app downloads and usage over time."[31]

43. Thus, Apple intentionally cultivates an impression of trustworthiness amongst consumers, including that apps on the App Store are highly vetted and safe for users to download and use.[32] "The more consumers trust a brand, the more they use that brand. . . . Apple's huge installed base of trusting users has tremendous value, driving a high level of spend with the brand."[33]

44. Because Plaintiff knew, or at least thought she knew, that Apple thoroughly reviews applications before it allowed them on the App Store, and in reliance on Apple's representations that App Store apps are safe and secure, Plaintiff purchased Apple hardware (i.e., an iPhone) and downloaded the Swiftcrypt app from the App Store, which turned out to be a fraudulent application.

45. The fraudsters that perpetrated the fraud against Plaintiff and Class members through the App Store did so specifically because the app being in the App Store would lend credibility to the scheme. The fraudsters knew that Apple advertises the App Store as being a safe and trustworthy platform, and they used those representations to their advantage in order to carry out the fraud.

---

[31] *See* Juliette Caminade & Jonathan Borck, *The Continued Growth and Resilience of Apple's App Store Ecosystem*, Apple (May, 2023), https://www.apple.com/newsroom/pdfs/the-continued-growth-and-resilience-of-apples-app-store-ecosystem.pdf.

[32] *See id.* ("Apple has heavily invested in the development of policies to foster user trust and the deployment of resources to enforce them.").

[33] David Myhrer, *How Brand Trust and a Strong Product Portfolio Drives Apple's Success*, IDC (Feb. 12, 201), https://blogs.idc.com/2021/02/12/how-brand-trust-and-a-strong-product-portfolio-drives-apples-success/.

Digital Asset Frauds

46. With Apple's representations in mind, Plaintiff downloaded the Swiftcrypt app, reasonably trusting that the app would be safe, legitimate, and suitable for conducting secure financial transactions. Instead, Plaintiff was met with digital asset fraud, finding herself a victim of a scheme that Apple's promises of safety should have prevented.

47. Fraudsters can carry out these digital asset frauds in different ways. One common mechanism is to "claim to invest customers' funds in proprietary crypto trading systems or in 'mining' farms. The fraudsters promise high guaranteed returns (for example, 20-50%) with little or no risk."[34]

48. Fraudsters can create fake "trading" platforms in which they convince persons to deposit money in what they believed was their own account under their control, often starting with small amounts and building up to higher and higher numbers, promising the users that they are trading their money and achieving high returns.[35] In reality, "no trading actually [takes] place."[36] Any money deposited into the platform is stolen by the scammers. "When [victims] try to withdraw [their] earnings, suddenly there [is a] problem[]," or they are told they must pay out-of-pocket to cover exorbitant undisclosed fees or fake taxes.[37]

49. These cryptocurrency scams are extremely prevalent. The FBI recently reported that the total amount of money lost in these frauds in 2023 was over $5.6 billion.[38] Investment scams,

---

[34] *Investor Alert: Watch Out for Fraudulent Digital Asset and "Crypto" Trading Websites*, Commodity Futures Trading Commission, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/watch_out_for_digital_fraud.html#:~:text=Be%20wary%20of%20anyone%20who,that%20is%20difficult%20to%20understand. (last accessed May 28, 2025).

[35] *See Digital Asset Frauds*, Commodity Futures Trading Commission, https://www.cftc.gov/LearnAndProtect/digitalassetfrauds (last accessed May 28, 2025).

[36] *Id.*

[37] *Id.*

[38] Hannah Lang, *Losses from Crypto Scams Grew 45% in 2023, FBI Says*, Reuters (Sept. 9, 2024 3:16pm CDT), https://www.reuters.com/technology/losses-crypto-scams-grew-45-2023-fbi-says-2024-09-09/.

such as the ones discussed above and at issue here, "accounted for 71% of all crypto-related losses" in 2023.[39] The U.S. Secret Service has warned that these types of frauds are of "national interest."[40]

50. Sophisticated digital actors, such as Apple, are well aware of the threat of these schemes. Apple knew, or should have known, that these types of frauds exist and should have protected Plaintiff and Class members against these types of frauds. Despite representations that Apple takes App Store security seriously, that its customers can trust what is available in the App Store, and that App Store apps used to trade cryptocurrency meet all relevant legal requirements, Apple allowed these fraudsters to place their apps for download in the App Store and caused great harm to Plaintiff and Class members.

Plaintiff Danyell Shin's Experience

51. In or about September, 2024, Plaintiff joined an online investment discussion group whose purported objective was to share stock recommendations, investment strategies, and to leverage the combined investment resources of the group. Plaintiff had been educating herself by various means regarding stock investments and trading of digital assets and the online discussion group was part of this process. At the behest of the group leader, an individual using the name Daniel Mills, who was a claimed financial expert with a pedigreed employment history, the Mills discussion group expanded into trading cryptocurrency. Plaintiff and the other group members were encouraged to download and join an app called Swiftcrypt from either the App Store or the Google Play Store and utilize the $100 to $2,000 provided by the exchange to start "trading."

52. Plaintiff has used Apple products for at least 15 years. She trusted apps from the App Store because of her experience with Apple products, her experience with downloading and using other apps from the App Store, and the overall impression Apple has cultivated among its customers—that apps on the App Store are vetted, safe, and trustworthy. This confidence arose from Apple's long-standing commitment to marketing the App Store as a secure platform, where all apps meet rigorous safety standards. She was also assured by Apple's representations on its App Store

---

[39] *Id.*

[40] *Combating the Illicit Use of Digital Assets*, United States Secret Service, https://www.secretservice.gov/investigations/digitalassets (last accessed May 28, 2025).

that its apps could be trusted and were secure and safe as alleged above. In reliance on this impression Apple has cultivated over time that apps on the App Store are vetted, safe, and trustworthy, including Apple's representations regarding the safety and security of App Store apps and based on her belief that the Swiftcrypt app downloaded from Defendant's App Store was safe and secure, Plaintiff downloaded Swiftcrypt onto her iPhone 13 Pro Max in or about September, 2024.

53. Plaintiff's reliance on Apple's representations was reasonable because the representations she relied on concern the safety and security of apps from the App Store—the "guiding principle" of the App Store according to Apple—and Plaintiff relied upon Apple's representations for these purposes. Plaintiff would not have purchased an iPhone or spent as much on her iPhone if she had known the truth about Apple's representations that its apps were not safe or trustworthy.

54. After relying on Apple's representations about the safety and vetting of apps in the App Store and downloading the Swiftcrypt app, Plaintiff began transferring money into what she believed was her account and buying and trading in cryptocurrency and Initial Coin Offerings (ICOs). Between September, 2024, and mid-January, 2025, Plaintiff transferred approximately $80,000 into the Swiftcrypt app, including approximately $50,000 obtained through a loan from her husband's 401k account. By mid-January, 2025, Plaintiff's Swiftcrypt account appeared to have increased to $421,000.

55. On or about January 14, 2025, Plaintiff's Swiftcrypt account was suddenly locked and her assets in her account frozen. A few days later, the Swiftcrypt app became non-functional and non-responsive. Plaintiff later discovered the Swiftcrypt app was not legitimate or in compliance with legal requirements, contrary to Apple's representations, it was not safe and could not be trusted, and it did not comport with Apple's represented standards and vetting processes for a cryptocurrency app. The Swiftcrypt app was part of a "pig butchering" scam and the more than $80,000 that Plaintiff had deposited was gone. As a direct result of Apple's process for reviewing the Swiftcrypt app on its App Store and Plaintiff's reasonable reliance on Apple's representations assuring her the app had been vetted, was safe, and could be trusted, Plaintiff was injured and lost approximately $80,000.

Contrary to Apple's representations and stated processes for correction, Plaintiff and other users of Swiftcrypt were never notified by Apple that Swiftcrypt was a dangerous app used for fraud and malicious activity. Because of the false and deceptive material misrepresentations at issue, Plaintiff also overpaid for her iPhone.

CLASS ACTION ALLEGATIONS

56. Plaintiff brings this action on behalf of herself and as a class action, pursuant to the provisions of Federal Rules of Civil Procedure Rules 23(a), (b)(2), and (b)(3), on behalf of the class defined as:

The Class

> All persons who downloaded a cryptocurrency trading app from the Apple App Store within the relevant statutory period to the date notice is sent to the Class and whose funds were stolen from the cryptocurrency app by the app developers or agents working on their behalf.

57. Excluded from the Class are Defendant and its subsidiaries and related entities; all persons who make a timely election to be excluded from the Class; governmental entities; and any judge to whom this case is assigned and his/her immediate family. Plaintiff reserves the right to revise the Class definition based upon information learned through discovery.

58. Certification of Plaintiff's claims for class-wide treatment is appropriate because Plaintiff can prove the elements of her claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claim.

59. This action has been brought and may be properly maintained on behalf of the Class proposed herein under Federal Rule of Civil Procedure 23 for the following reasons:

Numerosity

60. Pursuant to Federal Rule of Civil Procedure 23(a)(1), the members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are hundreds of members of the Class, the precise number of Class members is unknown to Plaintiff but may be ascertained from Defendant's records. Class members may effectively and efficiently be notified of the pendency of

this action by recognized, Court-approved dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or publication.

Commonality and Predominance

61. Pursuant to Federal Rule of Civil Procedure 23(a)(2) and 23(b)(3), this action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

a. Whether Defendant engaged in the conduct alleged herein;

b. Whether Defendant's conduct constituted violations of state consumer protection laws;

c. Whether Plaintiff and the other Class members are entitled to damages, restitution, or other monetary relief and, if so, in what amount; and

d. Whether injunctive relief is appropriate, including corrective advertising regarding the safety of App Store apps, and the form thereof.

Typicality

62. Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were injured through Defendant's wrongful conduct as described above.

Adequacy

63. Plaintiff is an adequate Class representative because her interests do not conflict with the interests of the other members of the Class she seeks to represent; Plaintiff has retained experienced counsel competent in complex multi-party and class action litigation, and Plaintiff intends to prosecute this action vigorously. The Class's interests will be fairly and adequately protected by Plaintiff and her counsel.

Superiority

64. Class action litigation is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this action as a class action. The damages suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to

individually litigate their claims against Apple, so it would be impracticable for members of the proposed Class to individually seek redress from the courts. Even if the individual Class members could afford to undertake individual litigation, such individual claims would unnecessarily burden the court system should they do so. Furthermore, individual litigation creates potential for inconsistent or contradictory orders and judgments and increases delay and expense to the parties and to the court system. A class action would present fewer administrative difficulties, would be more efficient, and would enhance the interests of consistent and fair justice in this matter.

65. In the alternative, the Class also may be certified because Defendant has acted or refused to act on grounds generally applicable to the Class thereby making final declaratory and/or injunctive relief with respect to the members of the Class as a whole, appropriate.

66. Plaintiff seeks preliminary and permanent injunctive and equitable relief on behalf of the Class, on grounds generally applicable to the Class, to enjoin and prevent Defendant from engaging in the acts described, and to require Defendant to provide relief to Plaintiff and Class members.

67. Unless the Class is certified, Defendant will retain monies that were taken from Plaintiff and Class members as a result of Defendant's wrongful conduct. Unless a classwide injunction is issued, Defendant will continue to commit the violations alleged and the members of the Class and the general public will continue to be misled.

COUNT I

Violations of the Unfair Competition Law,
Cal. Bus. & Prof. Code § 17200, *et seq.*

68. Plaintiff repeats and incorporates herein by reference the allegations in the preceding paragraphs of this complaint, as if set forth fully herein.

69. Plaintiff and Defendant are "persons" within the meaning of the UCL. Cal. Bus. & Prof Code § 17201.

70. The UCL defines unfair competition to include any "unlawful, unfair, or fraudulent business act or practice." Cal. Bus. & Prof Code § 17200.

71. As a result of engaging in the conduct alleged in this Complaint, Defendant has violated the UCL's proscription against engaging in "unlawful" conduct by virtue of its violations of California's Consumers Legal Remedies Act, Civil Code § 1750, violation of Civil Code §§ 1572, 1573, 1709, 1711, 1770(a)(5), (7), (9) and the common law. Plaintiff reserves the right to allege other violations of law which constitute unlawful business acts or practices under the UCL.

72. As a result of engaging in the conduct alleged in this Complaint, Defendant has also violated the UCL prohibition against unfair business acts or practices. Defendant's unfair conduct alleged in this Complaint is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers because consumers have lost substantial amounts of money using App Store apps that were not legitimate, vetted, or safe as represented by Apple. There is no utility or legitimate business purpose for Apple's conduct in that Apple by its express representations and long-term campaign promises that apps from its App Store are legitimate, safe, and secure and can be downloaded with confidence because of Apple's vetting process and security standards. However, because Apple has prioritized profit over ethics, Apple fails to adequately vet predatory, potentially devastating "pig butchering" cryptocurrency scam apps and makes them available to download despite its continuing misrepresentations that the apps in its App Store are vetted, safe and trustworthy.

73. Apple's unfair conduct also undermines public policies aimed at protecting consumers from harm, especially in digital marketplaces. California, in particular, has a strong public policy in favor of safeguarding consumers against deceptive practices and ensuring that products and services available to the public do not pose undue risk of fraud or financial loss. Public policy encourages protecting citizens from financial scams and fraudulent schemes, particularly in digital markets where consumers are more vulnerable. By allowing fraudulent apps that facilitate "pig butchering" scams, Apple's conduct violates public policy aimed at preventing fraud and financial exploitation. Public policies also generally uphold the importance of transparency and truthfulness in advertising, especially when companies make safety and security claims. Apple's representations of App Store safety create a misleading sense of security, and violate policies against false advertising. There is also a public policy interest in maintaining high standards of digital security and privacy for consumers. Particularly given its representations to the contrary, Apple's

failure to vet fraudulent cryptocurrency trading apps contravenes public policies intended to ensure that digital services, especially those related to finance, do not expose users to unnecessary risk. Public policy supports the principle that companies with substantial market control have a duty to protect users from known risks, especially where users cannot avoid these risks themselves. Apple's exclusive control over iOS app distribution heightens its duty to protect consumers, and its failure to do so conflicts with public policies focused on consumer protection in monopolized digital markets.

74. Defendant's business practices are also unfair within the meaning of the UCL because the injury to Plaintiff and the Class is not outweighed by any countervailing benefits to consumers or competition, and the injury could not reasonably be avoided by Plaintiff and the Class members. There were reasonable available alternatives to further Defendant's legitimate business interests other than the conduct described herein.

75. As a result of engaging in the conduct alleged in this Complaint, Defendant has also violated the UCL prohibition against fraudulent business acts or practices by representing that apps from its App Store are legitimate, safe, and secure and can be downloaded with confidence because of Apple's vetting process and security standards. Defendant's conduct as set forth fully above was false, misleading, and/or likely to deceive a reasonable consumer. A reasonable consumer would be deceived or mislead by Apple's representations because the representations regarding the legitimacy, safety, and security of App Store apps are material to consumers' decision to purchase Apple hardware devices (iPhones and iPads) and download and use App Store apps for financial transactions and related purposes. Plaintiff and other Class members have in fact been deceived as a result of their reliance on Defendant's material misrepresentations.

76. Plaintiff has suffered injury in fact and lost money or property as a result of Defendant's unlawful, unfair, and fraudulent business acts and practices alleged herein. Because of the unfair business practices at issue, Plaintiff and members of the Class have suffered an injury in fact and have lost money and property, including, but not limited to, the expected utility and performance of their Apple iPhones and iPads, the purchase price of their Apple devices, and/or the difference between the price Class members paid and the actual worth of the hardware product had

Apple disclosed the true nature of the representations at issue. As a result of Defendant's misconduct and representations, Plaintiff also invested and lost thousands of dollars in a scam app she acquired through Apple's App Store.

77. Apple's conduct in violation of the UCL is ongoing and continuing to this date. The unlawful, unfair, and fraudulent business acts and practices of Defendant described herein present a continuing threat in that Apple is currently engaging in such acts and practices, and will persist and continue to do so unless and until an injunction is issued by this Court. Plaintiff intends to continue to purchase App Store apps in the future if they are secure and comport with Apple's claims regarding its standards, vetting, and review. Because Plaintiff owns Apple iPhones and/or iPads, and the ability to download and use apps is integral to the core functionality of the Apple devices she owns, she has no reasonable, comparable alternatives except to download and use apps from Apple's App Store. Injunctive relief, in the form of corrective advertising, is necessary to dispel public misperception about the safety and trustworthiness of apps in Apple's App Store that has resulted from years of Apple's unlawful marketing efforts and to prevent current and future Apple product users from being misled.

78. Plaintiff, on behalf of herself and the Class members, seeks restitution from Defendant of all money and property lost by Plaintiff and the other members of the Class investing through fraudulent cryptocurrency apps acquired through the App Store and by overpaying for their Apple hardware devices, an injunction prohibiting Defendant from continuing the unfair business practices, corrective advertising, and all other relief this Court deems appropriate, consistent with Business & Professions Code § 17203.

COUNT II

Violations of Consumers Legal Remedies Act,
Cal. Civ. Code § 1750, *et seq.*

79. Plaintiff repeats and incorporates herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

80. At all relevant times the Apple devices (e.g., iPhones or iPads), which include the App Store and applications available therein are goods or services that Apple has marketed and that

Plaintiff and Class members purchased or obtained for personal, family, or household purpose and, as such, are "goods" and "services" as defined by Cal. Civil Code sections 1761(a), (b).

81. Plaintiff and Class members are individuals who purchased or leased and have used one or more Apple devices (e.g., iPhones or iPads) for personal, family, or household purposes and, as such, are "consumers" defined in Cal. Civil Code section 1761(d). Apple is a corporation and, as such, is a "person" as that term is defined in Cal. Civ. Code section 1761(c).

82. Plaintiff and Class members purchased iPhones and iPads based at least in part on the mistaken belief and impression cultivated by Apple that the devices could be used to download safe and trustworthy apps vetted by Apple and available in the App Store, and that Apple does not permit apps that violate its developer guidelines (including requirements for safe and trustworthy cryptocurrency exchange apps). Plaintiff and members of the Class would not have purchased the Apple hardware devices and/or would not have paid as much for them if Apple disclosed that the representations discussed herein were false and misleading.

83. In offering apps for download in the App Store onto Apple devices (e.g., iPhones or iPads), Apple represented that applications downloaded from the App Store are safe for use on Apple devices. Apple represents, *inter alia*, that "the App Store has proved to be a safe and trusted place to discover and download apps," that Apple is"[d]edicated to trust and safety," that "Apps must adhere to our guidelines," that "[e]very week, over 500 dedicated experts around the world review over 100 Apps," and that "[o]ver 1M submissions rejected for objectionable, harmful, unsafe, or illegal content."[41]

84. As a result of these and other representations as alleged above, Plaintiff and Class members purchased iPhones and iPads and downloaded and used the fraudulent cryptocurrency apps from the App Store. A reasonable consumer would be deceived or mislead by Apple's representations because the representations regarding the legitimacy, safety, and security of App Store apps are material to consumers' decision to purchase iPhones and iPads and download and use App Store apps for financial transactions and purposes.

[41] *Supra* n.2.

85. Notwithstanding these representations, the cryptocurrency apps used by Class members were not legitimate, safe, or trustworthy and Defendant failed to properly vet the cryptocurrency applications before providing them to the public.

86. By virtue of this ongoing practice and course of conduct, Defendant has violated and will continue to violate section 1770(a)(2) of the CLRA by misrepresenting the source, sponsorship, approval, or certification of its goods or services.

87. By virtue of this ongoing practice and course of conduct, Defendant has violated and will continue to violate section 1770(a)(5) of the CLRA by representing that its goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have.

88. By virtue of this ongoing practice and course of conduct, Defendant has violated and will continue to violate section 1770(a)(7) of the CLRA by representing that its goods or services are of a particular standard, quality, or grade, when in fact, they are of another.

89. By virtue of this ongoing practice and course of conduct, Defendant has violated and will continue to violate section 1770(a)(9) of the CLRA by advertising goods with intent not to sell them as advertised.

90. Defendant's violations of the CLRA present a continuing threat to Plaintiff and Class members in that Defendant continues to engage in the above-referenced acts and practices, and unless enjoined from doing so by this Court, will continue to do so. Plaintiff intends to continue to download and use App Store apps in the future if they are secure and comport with Apple's claims regarding standards, vetting, and review. Because Plaintiff and Class members own Apple iPhones and/or iPads, and the ability to download and use apps is integral to the core functionality of the Apple devices they own, they have no reasonable, comparable alternatives except to download and use apps from Apple's App Store. Injunctive relief, in the form of corrective advertising, is necessary to dispel public misperception about the safety and trustworthiness of apps in Apple's App Store that has results from years of Apple's unlawful marketing efforts and to prevent current and future Apple product users from being misled. Defendant's conduct is fraudulent, wanton, and malicious.

91. In compliance with Civil Code section 1780(d), attached as **Exhibit A** is the affidavit showing that the action has been commenced in the proper forum.

92. Plaintiff seeks an order awarding equitable relief, as well as an award of attorneys' fees and costs pursuant to Civil Code § 1780 (a), (d) and (e). Plaintiff will amend her complaint to seek actual damages as provided by the CLRA if Apple does not take corrective action within thirty days of receiving notice of its violations of the CLRA.

COUNT III

Declaratory Relief

93. Plaintiff repeats and realleges all paragraphs as if fully set forth herein.

94. Pursuant to 28 U.S.C. § 2201, the Court "may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought."

95. An actual, present, and justiciable controversy exists between Plaintiff and Apple regarding the truth and legality of Apple's representations and omissions concerning the safety, legitimacy, and vetting of apps available in the App Store, including the apps used in the fraudulent schemes alleged herein.

96. Apple has publicly represented that apps from its App Store are legitimate, safe, and secure and can be downloaded with confidence because of Apple's vetting process and security standards.

97. Plaintiff and Class members downloaded and used such apps in reliance on Apple's representations and were harmed as a result.

98. Plaintiff, individually and on behalf of the other Class members, seek entry of the following declarations: (a) Apple's representations regarding the legitimacy, safety, vetting process and security standards as alleged herein were false or deceptive; and (b) Apple is liable for damages to Class members proximately caused by its false or deceptive representations.

///

///

///

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully prays for judgment against Defendant as follows:

A. For an Order certifying the Class;

B. For an Order declaring Defendant's conduct unlawful;

C. For preliminary and permanent injunctive relief prohibiting Defendant from committing in the future those violations of law herein alleged and for corrective advertising to inform users regarding Defendant's failure to comply with its vetting and review of App Store apps;

D. For damages and restitution to Plaintiff and to the Class as permitted by law and equity under the laws alleged herein;

E. For pre- and post-judgment interest according to proof;

F. For costs of suit, including reasonable attorney fees, costs, and expenses under applicable provisions of law;

G. For all other relief this Court deems just, equitable, and proper.

JURY DEMAND

Plaintiff hereby requests a jury trial for all issues triable by jury.

Respectfully submitted,

Dated: June 12, 2025

BLOOD HURST & O'REARDON, LLP
TIMOTHY G. BLOOD (149343)
LESLIE E. HURST (178432)
THOMAS J. O'REARDON II (247952)
ADAM M. BUCCI (327312)

By: *s/ Timothy G. Blood*
TIMOTHY G. BLOOD

501 West Broadway, Suite 1490
San Diego, CA 92101
Tel: 619/338-1100
619/338-1101 (fax)
tblood@bholaw.com
lhurst@bholaw.com
toreardon@bholaw.com
abucci@bholaw.com

BARNOW AND ASSOCIATES, P.C.
BEN BARNOW (*pro hac vice forthcoming*)

ANTHONY L. PARKHILL (*phv forthcoming*)
205 W. Randolph Street, #1630
Chicago, IL 60606
Tel: 312/621/2000
312/641-5504 (fax)
b.barnow@barnowlaw.com
aparkhill@barnowlaw.com

Attorneys for Plaintiff