Kiley L. Grombacher
Bradley Grombacher, LLP
31355 Oak Crest Drive, Suite 210
Westlake Village, CA 91361
Kgrombacher@bradleygrombacher.com
Telephone: 805-270-7100
Facsimile: 805-270-7589

Daniel J. Thornburgh (*pro hac vice*)
Reagan Charleston Thomas (*pro hac vice*)
Kimberly Tanner (*pro hac vice)*
AYLSTOCK, WITKIN, KREIS
& OVERHOLTZ, PLC
17 East Main Street, Suite 200
Pensacola, FL 32502
dthornburgh@awkolaw.com
rthomas@awkolaw.com
ktanner@awkolaw.com
Telephone: 850-202-1010
Fax: 850-916-7449

Counsel for Plaintiffs

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

JAMES RAMIREZ, CHRISTOPHER ELLIS, JALEN DELGADO Plaintiffs, v. APPLE, INC. Defendants.	Case No. **<u>COMPLAINT FOR DAMAGES AND DEMAND FOR JURY TRIAL</u>**

Plaintiffs James Ramirez, Christopher Ellis, and Jalen Delgado, individuals, file their consolidated complaint against Apple, Inc. (Apple or Defendant), and in support thereof state:

INTRODUCTION

1. Plaintiffs James Ramirez, Christopher Ellis, and Jalen Delgado (collectively, "Plaintiffs") allege upon personal knowledge and information and belief, based upon, *inter alia*, the investigation made by and through their attorneys as to all other matters, as follows. This action arises from Apple, Inc.'s ("Apple" or "Defendant") negligent and misleading representations regarding the safety and integrity of its App Store, and from Apple's defective design, manufacture, and operation of the App Store platform, which Apple knew or should have known was being exploited by cybercriminals to steal funds from Apple's own customers.

2. For years, Apple has utilized the App Store as a gateway to draw consumers into its tightly controlled ecosystem, thereby driving sales of its hardware and related products. As part of a sustained marketing campaign, Apple has positioned itself, its products and services, as offering a level of security and trustworthiness superior to any competing technology company. This includes assurances about the safety of applications distributed through its App Store. By retaining exclusive control over which apps are permitted on Apple devices, Apple has structured its platform to ensure that consumers depend entirely on its promise of safety and reliability.

3. Apple has further, and repeatedly, represented that all apps available in the App Store are rigorously reviewed, trustworthy, and secure. These representations cultivate

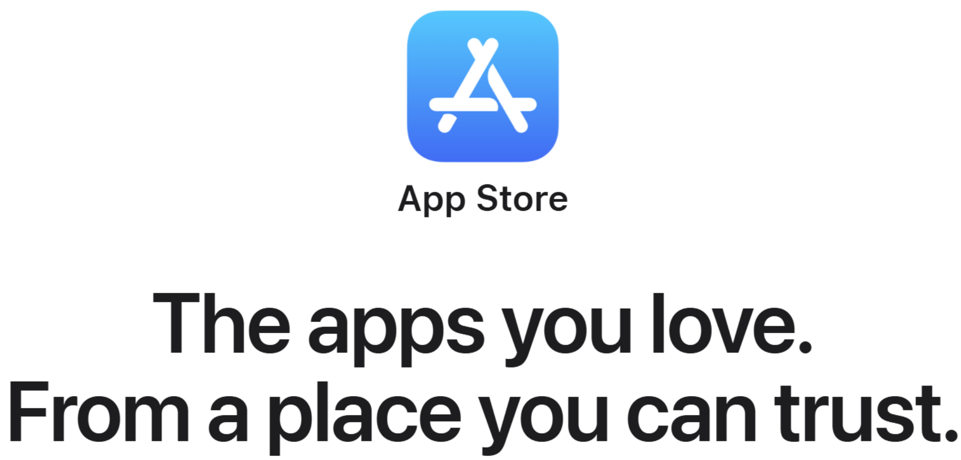
consumer confidence, which in turn motivates consumers to choose Apple devices over competing products and to obtain applications exclusively through the App Store, another significant revenue stream for Apple.

4. Despite its extensive marketing efforts, Apple has failed to devote the necessary attention and oversight to adequately review and monitor applications distributed through the App Store. This failure has allowed cybercriminals to exploit the trust, and reputation, Apple has cultivated, resulting in the theft of funds from Apple's own customers. Absent Apple's knowing participation and meaningful support, these cybercriminal schemes could not have been carried out or brought to completion.

5. Instead of implementing the protective practices it publicly promised, Apple elected to safeguard its long-standing marketing narrative. Apple knowingly facilitated fraud and allowed it to proliferate by leveraging its considerable marketing reach to continue representing that apps available on the App Store were vetted, safe, secure, and reputable. Even when victims reported fraudulent conduct, Apple routinely took little to no remedial action.

6. Plaintiffs relied on Apple's repeated assurances and long-standing marketing campaign portraying the App Store as a safe and trusted marketplace when they downloaded what appeared to be the legitimate Sparrow digital asset storage and trading application. In truth, the Sparrow app was a fraudulent spoof designed to steal funds by capturing users' account credentials and diverting their digital assets to cybercriminals. Users found their accounts had been wiped out and their cryptocurrency assets

transferred to the scammers' private wallets. This fraud succeeded precisely because Apple exploited the consumer trust it had deliberately cultivated through more than a decade of marketing the App Store as a uniquely safe and trusted environment.



[1]

7. These assurances, repeated across Apple's public-facing marketing and communications, fostered the widespread belief that all applications offered through the App Store were carefully reviewed, secure, and dependable. Despite knowing of ongoing fraudulent activity, Apple chose to withhold this information and continue reinforcing its safety narrative. In doing so, Apple intensified consumer reliance on its representations while undermining the very trust it had worked to establish.

[1] Apple, *About the App Store*, available at www.Apple.com/app-store (last accessed February 27, 2026).

> **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. All designed to help you discover your next favorite app with confidence.**

[2]

8. Apple's affirmative representations, along with the overall impression created by its long-standing marketing campaign, conveyed to consumers that applications available through the App Store, including and specifically the fraudulent Sparrow digital asset platform, could be trusted as safe and secure because Apple subjected the apps to a rigorous review and approval process. However, these representations were false and misleading. As a result of Apple's misstatements and its failure to take appropriate corrective or preventive measures, Plaintiffs were induced to download and use the fraudulent Sparrow app, which was designed solely to misappropriate users' funds, causing substantial financial losses.

9. Through this action, Plaintiffs seek compensatory, treble, and punitive damages, injunctive relief, and all other appropriate relief to redress the injuries they have suffered as a direct result of Apple's misconduct, including claims sounding in strict products liability, negligence, negligent misrepresentation, fraud, and violations of the Consumers Legal Remedies Act ("CLRA"), Cal. Civ. Code § 1750 et seq.

---

[2] *Id.*

PARTIES

I. Plaintiffs

10. Plaintiff James Ramirez is a natural person and resident of the State of Louisiana. Plaintiff Ramirez downloaded the fraudulent Sparrow application from the Apple App Store in reliance on Apple's representations regarding the safety and trustworthiness of App Store applications. As a proximate result of Apple's misconduct, Plaintiff Ramirez suffered approximately $875,000 in losses when his digital assets were stolen through the fraudulent application**.** Plaintiff Ramirez has suffered severe financial harm, emotional distress, anxiety, and related injuries that persist to this day.

11. Plaintiff Christopher Ellis is a natural person and resident of the Commonwealth of Massachusetts. Plaintiff Ellis downloaded the fraudulent Sparrow application from the Apple App Store in reliance on Apple's representations regarding the safety and trustworthiness of App Store applications. As a proximate result of Apple's misconduct, Plaintiff Ellis suffered approximately $840,000 in losses when his digital assets were stolen through the fraudulent application. Plaintiff Ellis has suffered severe financial harm, emotional distress, anxiety, and related injuries that persist to this day.

12. Plaintiff Jalen Delgado is a natural person and resident of the Commonwealth of Massachusetts. Plaintiff Delgado downloaded the fraudulent Sparrow application from the Apple App Store in reliance on Apple's representations regarding the safety and trustworthiness of App Store applications. As a proximate result of Apple's misconduct, Plaintiff Delgado suffered approximately $120,000 in losses when his digital assets

were stolen through the fraudulent application. Plaintiff Delgado has suffered severe financial harm, emotional distress, anxiety, and related injuries that persist to this day.

II. **Defendant**

13. Apple, Inc. ("Apple" or "Defendant") is a multinational technology corporation incorporated in the State of California, with its principal place of business at One Apple Park Way, Cupertino, California. Apple designs, develops, and sells consumer electronics, software, and online services, including the Apple App Store. Apple reported approximately $416 billion in net sales for its 2025 fiscal year. Apple operates one of the world's largest mobile application marketplaces through its App Store, which offers millions of apps to over a billion users globally.

JURISDICTION AND VENUE

14. This Court has diversity jurisdiction over this action pursuant to 28 U.S.C. § 1332(a) because the matter in controversy exceeds $75,000, exclusive of interest and costs, and is between citizens of different states.

15. This Court has personal jurisdiction over Apple because Apple has purposefully availed itself of the privileges and protections of this forum through its acts and omissions. These include, without limitation, maintaining its principal place of business within this District, marketing and advertising its products and services to consumers in this District, selling those products and services to residents of this District, and otherwise conducting substantial business activities here.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391(b) because Apple maintains its principal place of business in this judicial district. Additionally, a substantial portion of the events, acts, and omissions giving rise to the claims asserted herein occurred within this District.

DIVISIONAL ASSIGNMENT

17. Pursuant to Civil Local Rule 3-2(c) of the United States District Court for the Northern District of California, Plaintiffs state that this civil action is properly assigned to the **San Jose Division**. This action is properly assigned to the San Jose Division because Defendant Apple Inc. maintains its principal place of business at One Apple Park Way, Cupertino, California 95014, which is located within Santa Clara County. Plaintiffs further allege that venue is proper in this District because a substantial portion of the events, acts, and omissions giving rise to Plaintiffs' claims occurred within this District.

18. Accordingly, assignment to the **San Jose Division** is proper under Civil Local Rule 3-2(c).

COMMON ALLEGATIONS TO ALL PLAINTIFFS

A. Cryptocurrency and Internet Scams – A Global Crisis

19. According to the Federal Bureau of Investigation's most recently published IC3 Report, United States consumers in suffered $9,322,335,911 in losses as a result of cryptocurrency scams.[3]

20. Cryptocurrency crime is a global crisis. Per Chainalysis, a leading cryptocurrency tracing organization, cryptocurrency fraud, resulted in global losses totaling at least 17 billion dollars.[4]

21. While the 2025 Apple App Store Fraud Report claims Apple prevented over 2 billion in fraud, it does not disclose the amount of actual fraud losses.[5]

B. Scope and Dominance of Apple's App Store

22. Apple operates one of the world's largest and most prominent mobile and tablet application marketplaces through its widely recognized App Store, offering millions of apps to over a billion users globally. It is likewise one of the most valuable and best-known corporations in the world, with an estimated 2025 global brand value exceeding hundreds of billions of dollars and consistently ranking as the top or among the top global brands—reflecting enormous financial resources and extensive goodwill built over decades of carefully managed branding and marketing.

[3] Internet Crime Complaint Ctr., Fed. Bureau of Investigation, 2024 IC3 Annual Report (2024), https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[4] Chainalysis, 2026 Crypto Crime Report: Scams (Jan. 12, 2026), https://www.chainalysis.com/blog/crypto-scams-2026/.[chainalysis]

[5] Apple Inc., The App Store prevented more than $9 billion in fraudulent transactions (May 26, 2025), https://www.apple.com/newsroom/2025/05/the-app-store-prevented-more-than-9-billion-usd-in-fraudulent-transactions/.[apple]

23. Apple reported approximately $416 billion in net sales in the 2025 fiscal year, reflecting continued year-over-year revenue growth and reinforcing its position as one of the world's largest, and most profitable, technology companies. Public filings and earnings statements emphasize that their prominent financial performance is driven by a combination of hardware (including iPhone, Mac, iPad, and wearables) and an expanding services ecosystem, such as the App Store, cloud services, and digital content.[6]

24. Last year, "[t]he App Store alone saw over 850 million average weekly users globally, with developers earning over $550 billion on our platform since 2008."[7]

25. Apple boasts that they:

> [i]nvest every day to ensure the App Store remains a safe and trusted place for users to find great apps. This consumer trust led to unprecedented engagement on the App Store in 2025, with over 850 million average weekly users spanning 175 countries and regions, helping developers grow their businesses and reach new customers around the world with the click of a button.[8]

---

[6] Forbes, *Apple's Desperate Pivot From Glass To Dopamine*, available at https://www.forbes.com/sites/jonmarkman/2026/01/13/apples-desperate-pivot-from-glass-to-dopamine/ (last accessed February 27, 2026).

[7] Apple, *2025 Marked a Record Breaking Year for Apple* Services, available at https://www.apple.com/newsroom/2026/01/2025-marked-a-record-breaking-year-for-apple-services/ (last accessed Mar. 2, 2026).

[8] *Id.*

26. Apple has invested heavily in cultivating this "consumer trust". It meticulously crafted its reputation as the operator of one of the safest, most expansive, and influential digital marketplaces in the world through the Apple App Store. As of early 2026, the App Store hosted approximately 1.96 to 2.095 million live applications available for download, underscoring the vast scale and reach of Apple's app ecosystem.[9]

27. This year alone, it is projected that 38 billion apps will have been downloaded from Apple's App Store, representing a 15% increase over the last five years.[10]

C. Apple's Trust-and-Safety Marketing Campaign

28. For years, Apple has sought to build and promote a reputation for offering applications that are carefully vetted, safe, and worthy of consumer trust. Through a long-running, consistent, and wide-reaching marketing and communications campaign, Apple cultivated the image that its App Store is a tightly curated marketplace where every app is subjected to a rigorous review to ensure compliance with Apple's safety, security, and privacy standards. This campaign effectively created and reinforced the overall impression, and corresponding consumer belief, that apps obtained from the App Store are, by default, secure and trustworthy.

29. According to Apple,

> [b]y reviewing every app before it becomes available on the App Store

---

[9] Apptunix, *Apple App Store Statistics*, available at https://www.apptunix.com/blog/apple-app-store-statistics/ (last accessed February 27, 2026).

[10] Electronic Team Inc., *Apple's App Store Key Stats and Insights You Need to Consider in 2025*, available at https://mac.eltima.com/app-store-stats/ (last accessed February 27, 2026).

> to help ensure it's free of malware and accurately represented to users, and by swiftly removing apps from distribution if they are found to be harmful and limiting the spread of future variants, Apple protects the security of the ecosystem and provides peace of mind to customers.[11]

30. Apple's messaging that apps on the platform are safe and secure is embedded in the very structure of its business model. Apple maintains exclusive control over app distribution on iOS devices and prohibits alternative app sources or "sideloading," thereby positioning the App Store as the sole authorized channel for obtaining apps on iPhones and iPads. In a 2021 white paper analyzing sideloading risks, Apple asserted that allowing apps to be installed outside the App Store would weaken or "cripple" iPhone privacy and security protections, exposing users to serious security threats—reinforcing a broader, long-term message that apps obtained through the Apple-approved App Store are the trustworthy and secure option for consumers.[12]

31. Apple's exclusive control over app distribution on its devices, and its longstanding refusal to permit sideloading, has been promoted as an intentional safeguard to protect users from unsafe, fraudulent, or malicious applications. Since the inception of the App Store, Apple held itself as a gatekeeper that would allow only safe and trustworthy apps to reach consumers. At the March 6, 2008, iPhone event introducing the App Store,

---

[11] Apple, *About Apple App Store* Security, available at https://support.apple.com/guide/security/about-app-store-security-secb8f887a15/web (last accessed February 27, 2026).

[12] Apple, *Building a Trusted Ecosystem for Millions of Apps*, available at https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf (last accessed February 27, 2026).

Steve Jobs underscored this principle by explaining that, although Apple and developers shared an interest in making as many apps available to users as possible, Apple would decline to distribute certain categories of applications, including pornographic, malicious, or privacy-invasive app: categories reinforcing Apple's commitment to screening out dangerous or untrustworthy software.

32. Apple consistently used public statements by senior executives to convey the message that only secure, vetted applications would be available to iPhone users. In 2007, Apple CEO Steve Jobs described Apple's mission for the platform as building an advanced system that would give developers broad, native access to the iPhone software environment while simultaneously protecting users from malicious programs and similar threats.[13]

33. In a 2009 media interview, Apple marketing executive Phil Schiller, likewise, represented that Apple built an App Store "that people can trust," emphasizing that users and their families could download applications with confidence that those apps would function as expected and not compromise security.[14]

---

[13] Adam Engst, *Steve Jobs's iPhone SDK Letter*, TidBits (Oct. 17, 2007), available at https://tidbits.com/2007/10/17/steve-jobss-iphone-sdk-letter/ (last visited Feb. 27, 2026).

[14] Jason Kincaid, *Phil Schiller Grants Interview About Apple's App Store, Claims Devs Actually Like Approval Process*, TechCrunch (Nov. 23, 2009), available at https://techcrunch.com/2009/11/23/phil-schiller-grants-interview-about-apples-app-store-claims-devs-actually-like-approval-process/ (last visited Feb. 27, 2026).

34. In 2010, Steve Jobs routinely publicly characterized the App Store as a curated platform subject to Apple's oversight and control which was designed to ensure that customers receive only high-quality applications in a secure environment.[15]

35. In 2011, commentators observed that Apple maintained a puritanical attitude toward its App Store, promoting the idea that "nothing sinful gets in" --holding itself out as a strict gatekeeper, even as security researchers were identifying bugs and vulnerabilities that exposed users to potential security flaws.[16]

36. Over the next decade, Apple continued to build on this puritanical posture, repeatedly reinforcing the notion that the App Store was a tightly controlled environment in which only safe, carefully screened apps were permitted to reach users.[17]

37. As set forth in Apple's 2021 whitepaper titled *Building a Trusted Ecosystem for Millions of Apps*, Apple "built industry-leading security protections into the device, and we created the App Store, a trusted place where users can safely discover and download apps."[18]

---

[15] Wired, *Apple Answers Questions About App Rejections, Raises Others* (Sep. 9, 2010), available at https://www.wired.com/2010/09/apple-review-guidelines/ (last visited March 2, 2026).

[16] Forbes, *iPhone Security Bug Lets Innocent-Looking Apps Go Bad* (Nov. 7, 2011), available at https://www.forbes.com/sites/andygreenberg/2011/11/07/iphone-security-bug-lets-innocent-looking-apps-go-bad/ (last visited March 2, 2026).

[17] Craig Federighi, Web Summit, *Apple Keynote: Privacy and Security*, YouTube (Nov. 2021), available at https://www.youtube.com/watch?v=f0Gum8UkyoI&t=92s (last accessed Mar. 2, 2026).

[18] Apple, *Building a Trusted Ecosystem for Millions of Apps: The Important Role of App Store Protections* (June 2021), available at https://www.apple.com/privacy/docs/Building_a_Trusted_Ecosystem_for_Millions_of_Apps.pdf (last accessed Mar. 2, 2026).

38. According to Apple, "[o]n 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."[19]

39. To provide its consumers the utmost peace of mind, Apple represented it "review[s] 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."[20]

40. In that same white paper, Apple effectively casts "sideloading" as the proverbial big, bad wolf that iPhone users should fear – portraying outside distribution channels as the primary source of scammers, malware, and ransomware –while assuring consumers that apps obtained through Apple's own rigorously vetted App Store are the ones they can trust.[21]

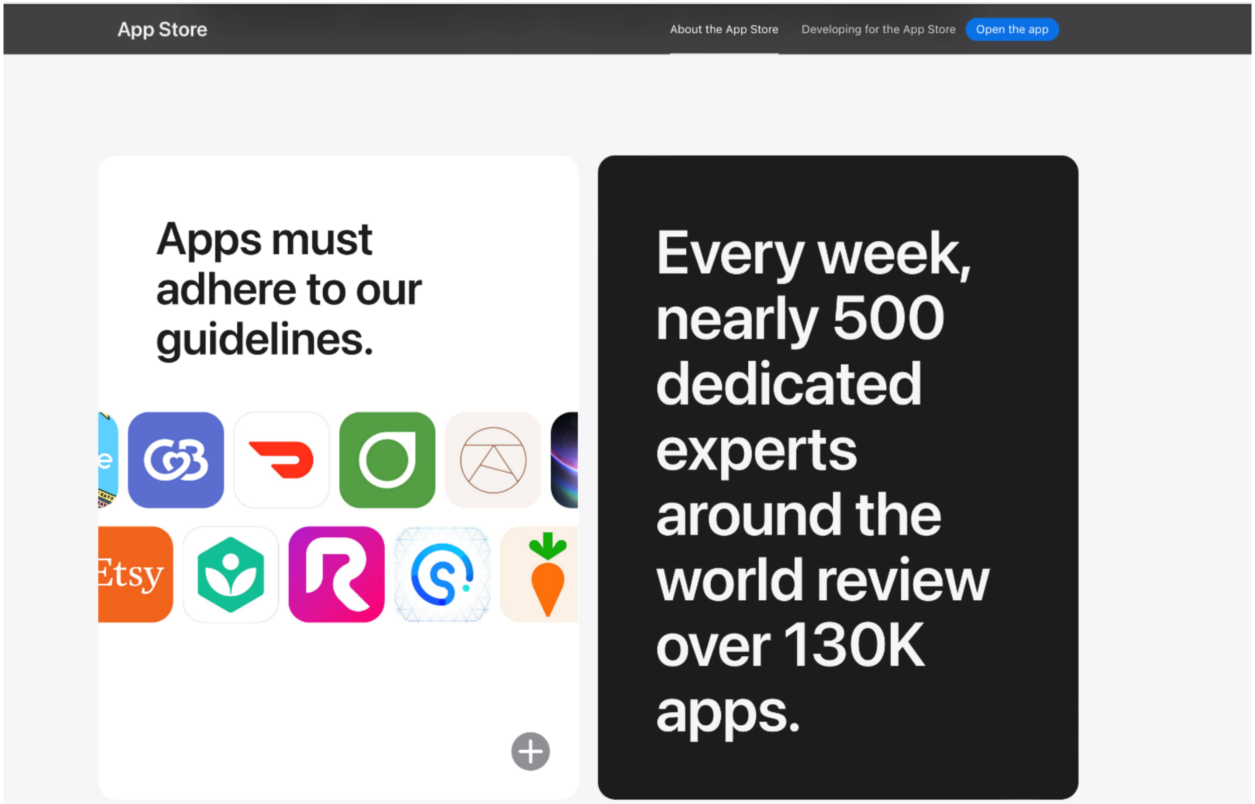
41. To this very day, Apple continuously touts the safety of its App Store, holding it out to be a curated platform with applications reviewed by its experts.

42. According to Apple, "[f]or 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. All designed to help you

---

[19] *Id.*
[20] *Id.*
[21] *Id.*

discover your next favorite app with confidence."[22]



[23]

43. Apple's current App Store landing page affirmatively represents that, for more than a decade, the App Store has been a "safe and trusted place" to discover and download apps and that all apps are held to the "highest standards for privacy, security, and content," such that users can download with confidence.[24]

44. According to Apple, "Apple maintains the safety of the App Store by ensuring every app is reviewed by a member of the App Review team. App submissions are reviewed

[22] Apple, *About the App Store*, available at https://www.apple.com/app-store/ (last accessed Mar. 2, 2026).
[23] *Id.*
[24] *Id.*

to help verify they meet Apple's high standards for privacy, security, and safety — consistent with the App Review Guidelines."[25]

45. Apple states that privacy and security are "built into everything we do," that 100% of apps are automatically screened for known malware, that apps cannot access data from other apps, and that dedicated reviewers assess hundreds of thousands of apps each week to enforce these standards.[26] Emphasis is placed on driving home the idea that the App Store is a safe place and that Apple is the watchful and vigilant eyes upon whom consumers can rely on.

46. Apple further emphasizes that it is "dedicated to trust and safety," touting its rejection of large numbers of app submissions for privacy, fraud, and other policy violations, removal of deceptive reviews, and availability of secure purchase mechanisms and refunds--all reinforcing the message that Apple's vetting, curation, and oversight make the App Store a safe, trustworthy environment for consumers.[27]

47. Apple represents the App Store as a safe, trusted marketplace where consumers can download apps with confidence, emphasizing that its review processes, malware screening, and fraud-prevention measures protect users from malicious or deceptive software.

---

[25] Apple, *Maintaining a Safe App Store Experience* (Sep. 15, 2025), available at https://support.apple.com/en-us/122712 (last accessed Mar. 2, 2026).
[26] *Id.*
[27] *Id.*

48. In public statements, Apple highlights billions of dollars in blocked fraudulent transactions and describes the App Store as a place where apps are carefully vetted, reinforcing the message that users can install apps with peace of mind.[28]

> **Newsroom** Apple Services Apple Stories Search Newsroom
>
> **App Review**
>
> Before any app makes its way onto the App Store, it is vetted by a member of Apple's App Review team, all of whom are deeply familiar with the App Review Guidelines, and focused on ensuring apps meet Apple's standards for quality and safety. On average, this team reviews nearly 150,000 app submissions each week, helping bring new apps and updates to the App Store. Last year, App Review helped more than 220,000 developers publish their first app on the App Store.

[29]

49. Each of these assurances reinforces the central theme of Apple's marketing: that its vetting process protects consumers from unsafe and fraudulent applications. Apple encourages consumers to rely on the premise that obtaining apps from the App Store is inherently secure. Apple continues to make these representations while approving and distributing fraudulent apps that it knows or should know do not meet its stated standards or its trust-and-safety commitments. Further, Apple fails to take meaningful action after receiving consumer complaints about fraudulent applications. In misrepresenting the safety of its store, Apple undermines and betrays the very trust it has worked for over a decade to cultivate.

---

[28] Apple, *The App Store Prevented More than 9 Billion in Fraudulent* Transactions (May 27, 2025), available at https://www.apple.com/newsroom/2025/05/the-app-store-prevented-more-than-9-billion-usd-in-fraudulent-transactions/ (last accessed Mar. 2, 2026).

[29] *Id.*

50. The safety and trustworthiness of Apple's App Store is the thread that is woven through its branding, FAQ, marketing, and ethos; however, at all relevant times, Apple knew or should have known that its negligent representations regarding the safety of its App Store placed its consumer base at risk because bad actors regularly and routinely were permitted to successfully submit their fraudulent applications to the App Store for download by unsuspecting and trusting Apple App Store Consumers.

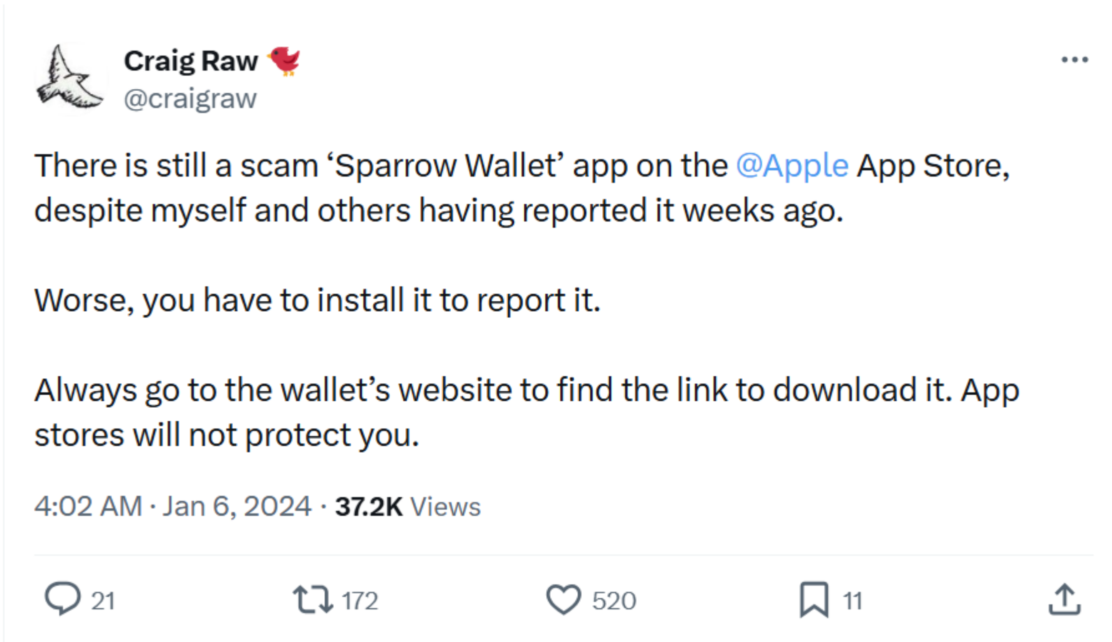
51. Despite these affirmative outward representations that apps in the Apple App Store are vetted by Apple experts and that the App Store is a safe and protected ecosystem, Apple buries disclaimers to the contrary deep within its click through terms and conditions.

52. Apple knew or should have known that consumers would rely on their prolific outward safety representations to their detriment. Apple further knew or should have known that users would rely on the outward and public statements and that any disclaimers buried in terms and conditions were unlikely to meaningfully reach its consumers.

53. Apple knew or should have known that its negligent representations would induce consumers to download applications from the App Store that exposed them to the risk of data breaches and financial loss.

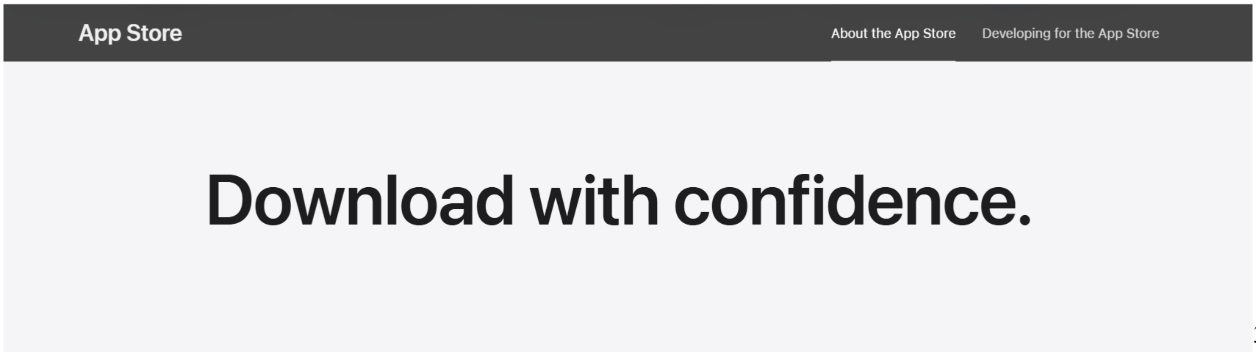
54. Apple knew or should have known that its App Store hosted fraudulent Apps harmful to its users.

55. For instance, as early as 2024, the founder of the Sparrow Bitcoin Wallet, Craig Raw, publicly criticized Apple for allowing fake "Sparrow Wallet" scam apps to remain on the App Store even after he and others reported them, warning that these apps are designed to steal users' Bitcoin.



56. Since that report, multiple Sparrow scam applications have worked their way into the Apple App Store with users reporting large losses as a result of downloading the spoofed Sparrow App.

57. Nevertheless, Apple's messaging and marketing stayed the same.



[30]

D. APPLE KNEW THE APP STORE HOSTED FRAUDULENT APPLICATIONS

58. As early as 2024, the founder of the legitimate Sparrow Bitcoin Wallet, Craig Raw, publicly criticized Apple for allowing fake “Sparrow Wallet” scam apps to remain on the App Store even after he and others reported them, warning that these apps were designed to steal users’ Bitcoin. Since that report, multiple Sparrow scam applications have worked their way into the Apple App Store, with users reporting large losses.

59. Apple knew or should have known that its App Store hosted fraudulent applications harmful to its users. Apple knew or should have known that consumers would rely on its representations to their detriment. Apple knew or should have known that its representations would induce consumers to download applications from the App Store that exposed them to the risk of data breaches and financial loss.

60. Despite multiple customer complaints, reports, and Sparrow’s own CEO calling on Apple to remove the fraudulent Apps, Apple’s messaging and marketing has stayed the same with no remedial change. Furthermore, upon information and belief, Apple ranked

---

[30] Apple, *About the App Store*, https://www.apple.com/app-store/ (last accessed Mar. 3, 2026).

the Sparrow app and included it in curated cryptocurrency app collections for download, effectively recommending a fraudulent application to consumers alongside legitimate ones.

E. APPLE FAILED TO WARN CONSUMERS ABOUT THE RISK OF FRAUDULENT APPS IN ITS APP STORE

61. Despite multiple reports made to Apple that its App Store hosted fraudulent and dangerous applications, Apple failed to warn consumers that spoofed wallet apps, including fake Sparrow applications, had appeared in the App Store and posed a serious risk of theft of cryptocurrency, seed phrases, private keys, wallet credentials, and other sensitive account information.

62. Apple likewise failed to warn users that they should never enter a seed phrase, private key, wallet recovery phrase, or other credential into an application merely because the application appeared in the App Store, and failed to provide heightened or app-specific warnings for cryptocurrency applications despite the uniquely foreseeable and catastrophic risk of irreversible theft associated with those products.

63. After receiving reports and complaints concerning fake Sparrow-related applications and other scam cryptocurrency apps, Apple also failed to issue prompt post-distribution warnings, alerts, takedowns, interstitial notices, or other corrective communications reasonably calculated to inform consumers of the danger and prevent additional losses.

64. Apple knew or should have known that consumers would interpret an application's availability in the App Store as an indication that the application had been sufficiently reviewed and vetted for authenticity, safety, and legitimacy, particularly where Apple consistently represented that the App Store was a safe and trusted marketplace and that its review process protected users from malware, scammers, and fraudulent activity.

65. Notwithstanding that knowledge, Apple did not provide adequate warnings to users that App Store placement did not mean a cryptocurrency application (or any application for that matter) was authentic, verified, or safe, that spoof and fraudulent cryptocurrency applications had been submitted to and distributed through the App Store, or that users should independently verify the developer and publisher of any cryptocurrency wallet or trading application before downloading or using it.

66. Apple further knew or should have known that ordinary consumers, including Plaintiffs, would not appreciate that a cryptocurrency wallet application presented in Apple's curated App Store could be a spoof designed to capture credentials and immediately exfiltrate or divert digital assets to criminal actors.

67. Because Apple failed to warn consumers, including and specifically Plaintiffs Ramirez, Ellis, and Delgado, consumers downloaded fraudulent apps and suffered significant losses and injury.

68. Had Apple provided reasonable and adequate warnings and instructions, Plaintiffs would not have downloaded the spoof Sparrow application, would not have entered

sensitive wallet credentials into the application, would not have exposed their digital assets to theft, and would have avoided or substantially reduced their resulting injuries.

69. Apple's failure to warn consumers of the known and foreseeable risk of spoofed cryptocurrency applications in the App Store was a direct and proximate cause of Plaintiffs' losses, including the loss of cryptocurrency assets, loss of time, emotional distress, anxiety, and other economic and noneconomic damages to be shown at trial.

PLAINTIFF SPECIFIC ALLEGATIONS

A. Plaintiff Ramirez

70. Plaintiff Ramirez has used Apple products and services for over two decades.

71. Plaintiff Ramirez relied on Apple's prolific marketing representations that its App Store was safe and free from dangerous spoof apps.

72. Relying on Apple's representations that its App Store was safe and the apps hosted in the Apple App store had been vetted by experts, Plaintiff Ramirez downloaded the Sparrow app on July 25, 2025.

73. Plaintiff Ramirez entered his seed phrase as instructed by the app.

74. Plaintiff Ramirez, shortly thereafter, realized that his cryptocurrency had been transferred to a scammer and that the Sparrow App was not a legitimate Sparrow App as was presented in the App Store.

75. Plaintiff Ramirez immediately reported to Apple on July 25, 2025, that the Sparrow App was fraudulent and that 7.4 Bitcoin had been transferred out of his reach

into the developers' accounts. Thus, at that time, Apple had actual notice that the Sparrow App hosted in its App Store was fraudulent and caused substantial harm to its customer.

76. To date, no one from Apple has reached out to Plaintiff Ramirez regarding his initial July 25, 2025, or any subsequent, report regarding the Sparrow App.

B. <u>Plaintiff Ellis</u>

77. Plaintiff Ellis has used Apple products and services since at least 2008.

78. Plaintiff Ellis relied on Apple's prolific marketing representations that its App Store was safe and free from dangerous spoof apps.

79. Despite Plaintiff Ramirez's earlier complaint to Apple regarding the fraudulent app and his significant losses, Plaintiff Ellis found the Sparrow App in the App Store.

80. Relying on Apple's representations that its App Store was safe and the apps hosted in the Apple App Store had been vetted by experts, Plaintiff Ellis downloaded the Sparrow app on or around August 3, 2025, just over a week after Plaintiff had Ramirez had reported, and Apple was on notice, of the fraudulent Sparrow App and corresponding risk of tremendous risk Apple customers faced.

81. Plaintiff Ellis entered his seed phrase as instructed by the app.

82. Plaintiff Ellis, shortly thereafter, realized that his cryptocurrency had been transferred to a scammer and that the Sparrow App was not a legitimate Sparrow App as was presented in the App Store.

83. Ellis immediately reported the App and his loss to Apple.

C. Plaintiff Delgado

84. Plaintiff Delgado has used Apple products and services since at least 2010.

85. Plaintiff Delgado relied on Apple's prolific marketing representations that its App Store was safe and free from dangerous spoof apps.

86. Relying on Apple's representations that its App Store was safe and the apps hosted in the Apple App Store had been vetted by experts, Plaintiff Delgado downloaded the Sparrow app on or around May 1, 2025.

87. Plaintiff Delgado entered his seed phrase as instructed by the app.

88. Plaintiff Delgado, shortly thereafter, realized that 1.05033242 Bitcoin had not been stored in a legitimate Sparrow wallet, but was, instead, transferred to a scammer and that the Sparrow App was not a legitimate Sparrow App as it was presented in the App Store.

89. Because of Apple's prolific misrepresentations regarding the safety and vetting of the apps hosted in the Apple App Store, Plaintiffs Ramirez, Ellis, and Delgado have suffered significant losses and resulting injuries.

90. But for Apple's negligent and fraudulent misrepresentations, failure to warn, and the deceptive design of the App Store, Plaintiffs would not have suffered significant loss and resulting injuries.

COUNT I
VIOLATIONS OF CONSUMERS LEGAL REMEDIES ACT, CAL. CIV. CODE § 1750, *ET SEQ.*

91. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

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

93. Plaintiffs 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).

94. Plaintiffs 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. Plaintiffs also relied on the representations that Apple does not permit apps that violate its developer guidelines (including requirements for safe and trustworthy cryptocurrency apps). Plaintiffs 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.

95. In offering apps for download in the App Store on Apple devices (e.g., iPhones or iPads), Apple represented, by implication, and expressly through a long-term advertising campaign that applications downloaded from the App Store are safe for use on the Apple devices. For example, Apple represented, *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, nearly 500 dedicated experts around the world review over 130k apps," and that "more than 1.9M app submissions were rejected for reasons that include privacy violations and fraudulent activity."[31]

96. As a result of these and other implied and express representations, including Apple's long-term advertising campaign regarding the safety of its apps as alleged above, Plaintiffs purchased iPhones and iPads and downloaded and used scam cryptocurrency apps (including the Sparrow app) from the App Store.

97. The representations about the App Store apps safety and trustworthiness were material to Plaintiffs. Relying on these representations, Plaintiffs purchased Apple products then downloaded and used scam cryptocurrency apps (including the Sparrow app) from the App Store.

98. 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' decisions to purchase iPhones and iPads and download and use App Store apps for financial transactions and purposes.

99. As a direct and proximate result of Apple's misconduct and misrepresentations, including its substantial assistance and participation in the pig butchering frauds

[31] Apple, *About the App Store*, https://www.apple.com/app-store/ (last accessed Mar. 3, 2026).

perpetrated through the Apple App Store apps, Plaintiffs lost hundreds of thousands of dollars in scam apps they acquired through Apple's App Store.

100. Notwithstanding these representations, the cryptocurrency applications on the App Store were not vetted, legitimate, safe or trustworthy; ultimately, Defendant failed to properly vet cryptocurrency applications before providing them to the public.

101. Defendant was aware of the presence of these fraudulent, malicious applications on their App Store. In fact, Plaintiffs Ramirez and Ellis reported the fraudulent Sparrow application to Apple in July 2025 and August 2025, respectively. However, to date, Defendant has not responded to Plaintiffs reports. Furthermore, fraudulent Sparrow apps still exist in Apple's App Store. Meanwhile, Apple continues to market its App Store as a safe, secure, and expert-vetted platform.

102. 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.

103. 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 the goods or services provided by Apple have sponsorship, approval, characteristics, uses, benefits, or quantities which, in fact, they do not have.

104. 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 not.

105. 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 and services, but not selling or presenting those services as advertised.

106. The written notice alleging CLRA violations, including identifying the specific unlawful practices at issue, and demanded correction/cure was sent to Defendant's principal California office via Certified mail, return receipt requested. Defendant failed to adequately cure within the requisite 30 days.

107. Plaintiffs seek an order enjoining Apple pursuant to Civil Code § 1780 (a)(2) from its ongoing violations of the CLRA and ongoing failure to vet the safety, security and legitimacy of cryptocurrency trading apps available on the App Store. Defendant's violations of the CLRA present a continuing threat to Plaintiffs. Specifically, Plaintiffs own Apple products, including iPhones, and intend 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 Plaintiffs own Apple iPhones and/or iPads, combined with the fact that 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. Unfortunately, Defendant continues to engage in the above-referenced acts and practices; unless enjoined from doing so by this Court, Defendants will continue to engage in these same deceptive practices. If Apple is not enjoined from continuing its unfair business practices, Plaintiffs, and other consumers, will not know whether the App Store apps,

and especially financial apps, are safe, vetted and legitimate. These consumers, like Plaintiff, will be unable to safely use or download such apps in the future without subjecting themselves to other financial scams perpetrated via unvetted, scam App Store apps. 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 as well as to prevent current and future Apple product users from being misled.

108. Additionally, Plaintiffs seek actual damages, punitive damages, restitution of property, and any other relief this Court deems good and proper.

COUNT II

<u>VIOLATION OF THE LOUISIANA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION ("LUPTA") (LAW LA. REV. STAT. §51:1405, *et. al.*)</u>

109. Plaintiffs repeat and incorporate by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

110. At all relevant times, Plaintiff Ramirez was a natural person residing in Louisiana and was a "person" entitled to bring a private action under LUTPA.

111. At all relevant times, Plaintiff Ramirez was a consumer as defined in La. Rev. Stat. § 51:1402.

112. At all relevant times, Apple was engaged in the conduct of trade or commerce within the meaning of LUTPA by advertising, marketing, offering for sale, selling, licensing,

distributing, operating, and maintaining Apple devices, the App Store, and related digital goods and services for consumer use, including in Louisiana.

113. LUTPA declares unlawful unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce. La. Rev. Stat. § 51:1405.

114. Apple engaged in unfair and deceptive acts and practices by representing, expressly and through implication, that the App Store was a safe and trusted marketplace; that the apps available through the App Store were reviewed and vetted for fraud, malware, security, and safety; and that consumers could obtain and use apps from the App Store with confidence. However, Apple knew or should have known that spoofed, fraudulent, and malicious cryptocurrency applications had appeared on, and were being distributed through, the App Store.

115. Specifically, Apple engaged in unfair and deceptive acts and practices by omitting and failing to disclose material information to Louisiana consumers, including:

a. App Store placement did not necessarily mean that a cryptocurrency application was authentic, verified, or safe;

b. spoof and fraudulent cryptocurrency wallet applications had appeared in the App Store;

c. Apple's review and approval processes did not ensure that all cryptocurrency applications offered through the App Store were legitimate and non-fraudulent; and

d. consumers downloading purported cryptocurrency wallet or trading apps through the App Store faced a material risk of theft of digital assets and compromise of seed phrases, private keys, and wallet credentials.

116. Apple's conduct was unfair because it offended established public policy and was immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers.

117. Specifically, Apple's conduct was unfair as it involved fraud, deceit, and misrepresentation, leading reasonable consumers into believing that apps available through the App Store, including cryptocurrency applications, were vetted and safe when, in fact, that was not true.

118. Plaintiff Ramirez reasonably relied on Apple's deceptive acts, omissions, and representations when he used an Apple device, searched for, downloaded, and used what appeared to be a legitimate Sparrow cryptocurrency application from the App Store.

119. In fact, Apple intended that consumers, including Louisiana consumers like Plaintiff Ramirez, relied on its trust-and-safety messaging and App Store vetting representations when deciding whether to purchase Apple devices, use the App Store as the exclusive source of applications on those devices, and download financial and cryptocurrency applications from the App Store.

120. As a direct and proximate result of Apple's unfair and deceptive acts and practices, Plaintiff Ramirez suffered an ascertainable loss of money and movable property, including corporeal or incorporeal property, within the meaning of La. Rev. Stat. §

51:1409, including, but not limited to, the loss of cryptocurrency assets, loss of the benefit of the bargain in purchasing Apple devices and services marketed as part of a safe and trusted ecosystem, and other economic losses in amounts to be proven at trial.

121. Defendant was aware of the presence of these fraudulent, malicious applications on their App Store. In fact, Plaintiff Ramirez reported the fraudulent Sparrow application to Apple on July 25, 2025. However, to date, Defendant has not responded to Plaintiffs reports.

122. Apple's conduct was knowing, intentional, and in bad faith, and Apple persisted in its deceptive safety messaging despite notice of fraudulent cryptocurrency applications and consumer harm.

123. Pursuant to La. Rev. Stat. § 51:1409, Plaintiff Ramirez seeks recovery of actual damages, attorneys' fees, costs, and all other relief authorized by law.

124. The written notice alleging La. Rev. Stat. § 51:1409 violations, including identifying the specific unlawful practices at issue, and demanded correction/cure was sent to Defendant's principal California office via Certified mail, return receipt requested. Defendant failed to adequately cure within 30 days.

125. To the extent permitted by La. Rev. Stat. § 51:1409, and supported by proof, Plaintiff Ramirez further seeks enhanced treble damages for any unfair or deceptive conduct knowingly continued after legally sufficient notice.

COUNT III
VIOLATION OF MASSACHUSETTS GENERAL LAWS CHAPTER CH. 93A

126. Plaintiffs repeat and incorporate by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

127. At all relevant times, Plaintiffs Christopher Ellis and Jalen Delgado were natural persons residing in the Commonwealth of Massachusetts and were “persons” within the meaning of Mass. Gen. Laws ch. 93A.

128. At all relevant times, Apple was engaged in trade or commerce within the meaning of Mass. Gen. Laws ch. 93A by advertising, marketing, selling, distributing, licensing, operating, and maintaining Apple devices, the App Store, and related digital goods and services for consumer use, including in Massachusetts.

129. Specifically, Plaintiffs Ellis and Delagado purchased, used, and relied upon Apple devices and the App Store for personal, family, business, and/or household purposes.

130. Apple engaged in unfair and deceptive acts and practices in violation of Mass. Gen. Laws ch. 93A, § 2, by representing, expressly and through implication, that the App Store was a safe and trusted marketplace; that applications available through the App Store were reviewed and vetted for fraud, malware, security, and safety; and that consumers could download apps from the App Store with confidence. In actuality, Apple knew or should have known that spoofed, fraudulent, and malicious cryptocurrency applications had been and were being made available through the App Store.

131. Specifically, Apple engaged in unfair and deceptive acts and practices by omitting and failing to disclose material facts to Massachusetts consumers, including:

a. App Store placement did not necessarily mean a cryptocurrency app was authentic, verified, or safe;

b. spoof and fraudulent cryptocurrency wallet applications appeared in the App Store;

c. Apple's review process did not ensure that all cryptocurrency apps offered through the App Store were legitimate or nonfraudulent; and

d. consumers who downloaded purported crypto wallet or trading apps through the App Store faced a material risk of theft of digital assets and compromise of seed phrases, private keys, or wallet credentials.

132. Apple's representations and omissions were material because a reasonable consumer would consider the safety, legitimacy, and vetting of App Store applications important in deciding whether to purchase Apple devices, to use the App Store as the exclusive source of apps on those devices, or whether to download and use cryptocurrency applications involving substantial financial assets.

133. In fact, Plaintiffs Ellis and Delagado relied on Apple's deceptive acts, omissions, and representations when they used Apple devices, searched for, downloaded, and used what appeared to be a legitimate Sparrow cryptocurrency application from the App Store.

134. Apple intended that consumers, including Massachusetts consumers, would rely on its safety and vetting representations, in addition to the fact that Apple used those representations as part of a long-running marketing campaign cultivating consumer trust in the App Store and the broader Apple ecosystem.

135. As a direct and proximate result of Apple's unfair and deceptive acts and practices, Plaintiffs Ellis and Delagado suffered injury and a loss of money or property, including, but not limited to, the theft and loss of their cryptocurrency assets, the loss of the benefit of their bargain purchasing Apple devices and services marketed as part of a safe and trusted ecosystem, as well as other economic injuries in amounts to be proven at trial.

136. Apple's conduct was unfair in that it offended established public policy, was immoral, unethical, oppressive, unscrupulous, and caused substantial injury to consumers was not reasonably avoided and could not be outweighed by any countervailing benefits to consumers or competition.

137. Apple's conduct was deceptive in that it had the capacity and tendency to mislead reasonable consumers into believing that apps available through the App Store, including cryptocurrency applications, had been vetted and could be downloaded and used safely but, in fact, were not.

138. Apple's violations of Chapter 93A were willful and knowing. Apple's conduct was knowing, intentional, and in bad faith, and Apple persisted in its deceptive safety messaging despite notice of fraudulent cryptocurrency applications and consumer harm.

139. Defendant was aware of the presence of these fraudulent, malicious applications on their App Store. Specifically, Plaintiff Ellis reported the fraudulent Sparrow application to Apple on August 3, 2025. However, to date, Defendant has not responded to Plaintiffs reports.

140. At minimum, Apple refused to acknowledge or remedy its misconduct despite notice of fraudulent apps present in the App Store and reports of consumer harm. Apple's actions, or lack thereof, highlight Apple's reckless disregard for the misrepresentations made through Apple's long-running marketing campaign cultivating consumer trust, entitling Plaintiffs Ellis and Delgado to damages as permitted by Mass. Gen. Laws ch. 93A, § 9.

141. Pursuant to Mass. Gen. Laws ch. 93A, § 9, Plaintiffs Ellis and Delgado provided Apple with the required written demand for relief at least thirty days prior to commencing an action for damages under Chapter 93A, describing the unfair and deceptive acts complained of and the injuries suffered. The written notice alleging Chapter 93A violations, including identifying the specific unlawful practices at issue, and demanded correction/cure was sent to Defendant's principal California office via Certified mail, return receipt requested. Defendant failed to adequately cure within the required 30 days.

142. As a result of Apple's violations of Chapter 93A, Plaintiffs Ellis and Delgado seek actual damages or statutory damages as allowed by law, multiple damages as

appropriate, attorneys' fees, costs, equitable and injunctive relief, and such other relief as the Court deems just and proper.

COUNT IV
FRAUDULENT MISREPRESENTATION

143. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

144. Apple's marketing, promotions, and advertisements contained deceptive and misleading statements, implications, and portrayals that the App Store was safe, rigorously curated, and that applications were thoroughly vetted. Specifically, Apple highlights billions of dollars in blocked fraudulent transactions, describing the App Store as a place where apps are carefully vetted, reinforcing the message that users can install apps with peace of mind.[32]

145. In actuality, the App Store hosted and distributed fraudulent applications designed to steal consumers' funds, a fact Apple had long been aware of.

146. Apple's marketing, promotions, and advertisements failed to disclose that the App Store's review process had significant known limitations, that fraudulent applications had been repeatedly identified on the platform, and that Apple was aware of ongoing fraud perpetrated through App Store applications.

[32] Apple, *The App Store Prevented More than 9 Billion in Fraudulent* Transactions (May 27, 2025), available at https://www.apple.com/newsroom/2025/05/the-app-store-prevented-more-than-9-billion-usd-in-fraudulent-transactions/ (last accessed Mar. 2, 2026).

147. Apple's conduct was fraudulent and deceptive because its misrepresentations and omissions had the capacity to, and did in fact, deceive reasonable consumers including Plaintiffs.

148. Reasonable consumers, including Plaintiffs, would have found it material to their decisions that Apple's review process could not guarantee application safety, and that, as a result, the App Store hosted fraudulent applications.

149. Plaintiffs reasonably and justifiably relied on the misrepresentations and omissions. Relying on Apple's deceptive acts, omissions, and representations, Plaintiffs used Apple devices, searched for, downloaded, and used what appeared to be a legitimate Sparrow cryptocurrency application from the App Store.

150. Plaintiffs were injured as a direct and proximate result of Apple's fraudulent conduct as described. As a direct and proximate result of Apple's unfair and deceptive acts and practices, Plaintiffs suffered injury and a loss of money or property, including, but not limited to, the theft and loss of their cryptocurrency assets, the loss of the benefit of their bargain purchasing Apple devices and services marketed as part of a safe and trusted ecosystem, as well as other economic injuries in amounts to be proven at trial.

151. Plaintiffs' reliance on Defendant's omissions and misrepresentations was a substantial factor in causing Plaintiffs' harm. But for Apple's misrepresentations about the safety, security, and thoroughness of their App Store vetting process, Plaintiffs would have not downloaded and interacted with the spoof Sparrow application.

152. Wherefore, Plaintiffs demand judgment against Apple for compensatory and punitive damages, together with interest, costs of suit, attorneys' fees, and all such other relief as the Court deems proper.

COUNT V
FRAUDULENT CONCEALMENT

153. Plaintiffs incorporate by reference each preceding and succeeding paragraph as though set forth fully at length herein.

154. Apple had a duty to disclose material facts about the App Store to Plaintiffs.

155. Apple fraudulently and deceptively marketed the App Store to Plaintiffs as safe, rigorously reviewed, and trustworthy when Apple, in fact, knew that the App Store hosted and distributed fraudulent applications that had caused substantial harm to consumers.

156. Specifically, Apple concealed that:

(a) its App Store review process had known limitations that could not guarantee application safety;

(b) fraudulent cryptocurrency applications had been repeatedly identified on the App Store;

(c) Apple was aware of ongoing fraud perpetrated through App Store applications;

(d) Apple had received reports from consumers and developers identifying specific fraudulent applications, including the Sparrow application; and

(e) Apple had failed to take adequate remedial action in response to those reports.

157. Plaintiffs did not know of the facts that Apple concealed. Apple intended to deceive Plaintiffs and the public by concealing these facts.

158. Apple had a duty to accurately provide this information to Plaintiffs. In concealing this information, Apple breached its duty. Apple had ample opportunities to disclose these facts to Plaintiffs, through advertising, on its websites, through the App Store, and through other media such as responding to Plaintiffs reports regarding the presence of fraudulent apps. Instead, Apple chose to withhold this information and ultimately gained financially from this concealment.

159. Plaintiffs relied to their detriment on Apple's fraudulent omissions. Had Plaintiffs been adequately informed of the material facts concealed from them, they would not have downloaded the fraudulent Sparrow application.

160. Apple's fraudulent concealment was a substantial factor in causing harm to Plaintiffs as described herein. Plaintiffs were injured as a direct and proximate result of Apple's fraudulent conduct. But for Apple's misrepresentations about the safety, security, and thoroughness of their App Store vetting process, Plaintiffs would have not downloaded and interacted with the spoof Sparrow application.

161. Plaintiffs demand judgment against Apple for compensatory and punitive damages, together with interest, costs of suit, attorneys' fees, and all such other relief as the Court deems proper.

COUNT VI
NEGLIGENT MISREPRESENTATION

162. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

163. Apple represented for years that its App Store is a safe and trusted place to obtain apps for over a decade. This representation appears at the top of its website for the App Store. It touts its review of proposed apps, claiming that the company is "[d]edicated to trust and safety."[33]

164. Despite its many representations to consumers that the App Store is safe and trusted, Apple approved fraudulent apps on the App Store which are specifically designed to steal money from users of the apps. Moreover, Apple had actual notice its customers suffered substantial losses as a result of downloading these fraudulent applications.

165. Apple had no reasonable grounds for denying the existence of these applications on the App Store. Specifically, numerous customers, including the Plaintiffs, reported the existence of fraudulent applications and applications conducting pig-butchering schemes on the App Store, like the spoof Sparrow application.

166. Apple makes these representations with an intent to induce consumers to rely on these statements and use the App Store with confidence that they will not be harmed by

[33] Apple, *Maintaining a Safe App Store Experience* (Sep. 15, 2025), available at https://support.apple.com/en-us/122712 (last accessed Mar. 2, 2026).

fraudulent apps. This is demonstrated by Apple's dedication to intense marketing of the App Store as safe and trusted.

167. Plaintiffs justifiably relied on Apple's years-long representations regarding the App Store's safety. Apple has made the safety of the App Store its core marketing message regarding the App Store.

168. Because of Apple's misrepresentations, Plaintiffs suffered an injury in fact and have lost money and property, including, but not limited to, thousands of dollars in cryptocurrency stolen through scam apps, 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 Plaintiffs paid and the actual worth of the hardware product had Apple disclosed the true nature of the representations at issue.

169. Apple's fraudulent concealment was a substantial factor in causing harm to Plaintiffs as described herein. Plaintiffs were injured as a direct and proximate result of Apple's fraudulent conduct. But for Apple's misrepresentations about the safety, security, and thoroughness of their App Store vetting process, Plaintiffs would have not downloaded and interacted with the spoof Sparrow application.

170. Plaintiffs demand judgment against Apple for compensatory and punitive damages, together with interest, costs of suit, attorneys' fees, and all such other relief as the Court deems proper.

COUNT VII
STRICT PRODUCTS LIABILITY – FAILURE TO WARN

171. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

172. At all relevant times, the App Store, together with the iOS app-distribution environment integrated into Apple's iPhones and iPads, was a product placed into the stream of commerce by Apple. Such products were designed, controlled, maintained, marketed, and distributed for consumer use.

173. Apple knew or should have known that the App Store presented a substantial and non-obvious risk that fraudulent and spoof cryptocurrency applications could be submitted to, approved by, displayed in, and downloaded from the App Store by consumers seeking legitimate financial applications.

174. Apple further knew or should have known that consumers were likely to rely on Apple's repeated representations that the App Store was a "safe and trusted place" and that apps were reviewed for safety, security, fraud, and malware, particularly when selecting cryptocurrency wallet and trading applications involving the transfer and storage of highly valuable digital assets.

175. This risk presented a substantial danger that consumers would download a spoof cryptocurrency application from the App Store and suffer theft of their assets. This risk was reasonably foreseeable to Apple, because Apple had exclusive control over app distribution on iOS devices, prohibited ordinary consumers from obtaining iPhone applications from alternative sources, received reports from consumers, including

Plaintiffs, regarding fraudulent applications, and was on notice of fake Sparrow-related applications and similar crypto scam apps disseminated through its product.

176. Absent an adequate warning from Apple, ordinary consumers would not have recognized that an application made available through Apple's App Store, and presented within Apple's curated marketplace, could be fraudulent, unauthenticated, and designed for the purpose of stealing cryptocurrency assets.

177. Despite this knowledge, Apple failed to provide adequate warnings or instructions to Plaintiffs, including but not limited to warnings that:

a. App Store approval did not mean a cryptocurrency app was authentic, licensed, or safe;

b. spoof and fraudulent cryptocurrency wallet applications had appeared in the App Store;

c. consumers should not rely on App Store placement as confirmation of legitimacy, safety, or security;

d. consumers should independently verify the publisher of any crypto wallet or trading app before downloading or use; and

e. consumers should never enter seed phrases, private keys, or wallet-recovery credentials into an app solely because it appeared in the App Store.

178. Apple also failed to provide post-sale or post-distribution warnings after it knew or should have known that fraudulent Sparrow-related applications and similar crypto

scam apps were present on the App Store and posed an ongoing threat to users. Defendant was aware of the presence of these fraudulent, malicious applications on their App Store. Specifically, Plaintiffs Ramierz and Ellis reported the fraudulent Sparrow application to Apple in July and August 2025, respectively. However, to date, Defendant has not responded to Plaintiffs reports.

179. Because the App Store and the integrated app-distribution environment lacked adequate warnings and instructions, they were defective and unreasonably dangerous when used in an intended or reasonably foreseeable manner.

180. Plaintiffs used Apple devices and the App Store in a foreseeable manner by searching for, downloading, and using what appeared to be a legitimate Sparrow cryptocurrency application from Apple’s exclusive app marketplace in reliance on Apple’s safety and vetting representations.

181. Had Apple provided adequate warnings and instructions, Plaintiffs would not have downloaded the spoof application, would not have entered sensitive wallet credentials into the application, would not have transferred or maintained cryptocurrency in connection with that application, and would have avoided or materially reduced their losses.

182. Apple’s failure to warn was a substantial factor in causing Plaintiffs’ harm, including loss of cryptocurrency assets, loss of time, and resulting emotional distress and related noneconomic harm.

183. As a direct and proximate result of Apple's failure to warn, Plaintiffs suffered damages in an amount to be proven at trial.

184. Plaintiffs therefore seek all damages, restitution, equitable relief, injunctive relief, costs, interest, and such other relief as the Court deems just and proper.

COUNT VIII
NEGLIGENT FAILURE TO WARN

185. Plaintiffs repeat and incorporate herein by reference the allegations in the preceding paragraphs of this Complaint, as if set forth fully herein.

186. At all relevant times, Apple designed, developed, controlled, maintained, marketed, distributed, and operated the App Store and the integrated iOS app-distribution environment used by Plaintiffs on their Apple devices.

187. The App Store and Apple's app-distribution environment were dangerous, or were likely to be dangerous, when used in a reasonably foreseeable manner because spoofed and fraudulent cryptocurrency wallet and trading applications could be submitted to, approved by, and displayed in the App Store. These same dangers were then accessed by consumers seeking legitimate financial applications, then downloading the applications—in a reasonably foreseeable manner—ultimately creating a foreseeable risk of theft of digital assets and related harm.

188. Apple knew or reasonably should have known of that danger because Apple exercised exclusive control over app distribution on iOS devices and publicly held itself out as reviewing apps for fraud, malware, safety, and authenticity. Additionally, Apple

received reports and complaints from consumers, including Plaintiffs, concerning the presence of fraudulent applications on the App store, including the fake Sparrow-related applications, and similar crypto scam apps.

189. Apple knew or reasonably should have known that ordinary users would not realize the danger that an application made available within Apple's curated App Store and presented as available for download through Apple's exclusive ecosystem, could be a spoof or fraudulent cryptocurrency app designed to capture credentials and steal users' assets.

190. Apple failed to use reasonable care to adequately warn Plaintiffs of these dangers or to provide reasonable instructions for safe use of the App Store in connection with cryptocurrency applications.

191. Reasonable warnings and instructions would have included, at a minimum, disclosures that:

a) App Store availability did not mean that a cryptocurrency app was authentic, verified, or safe;
b) fraudulent and spoof cryptocurrency apps had appeared in the App Store;
c) users should independently verify the developer and publisher of any crypto wallet or trading app before downloading or using the app;
d) users should never enter seed phrases, private keys, or wallet recovery credentials into an app based solely on its presence in the App Store; and
e) heightened caution was required when using App Store apps for cryptocurrency storage, transfer, or trading.

192. A reasonably careful company, particularly one in Apple's position, would have provided such warnings and instructions, especially after receiving notice of scam applications and consumer complaints about the presence of scam applications. Such a reasonably careful company, particularly one in Apple's position, would have also issued post-distribution warnings, takedowns, alerts, interstitials, or other direct notices to consumers concerning the presence and risk of spoof cryptocurrency apps.

193. Apple's failure to provide adequate warnings and instructions was negligent and fell below the standard of care.

194. Plaintiffs used their Apple devices and the App Store in a reasonably foreseeable manner by searching for, downloading, and using what appeared to be a legitimate Sparrow cryptocurrency application from Apple's exclusive app marketplace in reliance on Apple's trust-and-safety representations.

195. Had Apple exercised reasonable care and provided adequate warnings or instructions, Plaintiffs would not have downloaded the spoof application, would not have input wallet credentials or recovery information into the application, and would not have suffered the theft of their cryptocurrency assets and related harms.

196. Apple's negligent failure to warn was a substantial factor in causing Plaintiffs' injuries, including but not limited to loss of cryptocurrency assets, overpayment for Apple devices and services marketed as part of a safe and trusted ecosystem, loss of time, emotional distress, anxiety, sleeplessness, and other consequential harm to be proven at trial. As a direct and proximate result of Apple's negligent failure to warn,

Plaintiffs suffered damages in an amount according to proof, including but not limited to loss of cryptocurrency assets, overpayment for Apple devices and services marketed as part of a safe and trusted ecosystem, loss of time, emotional distress, anxiety, sleeplessness, and other consequential harm to be proven at trial.

197. Accordingly, Plaintiffs seek all available legal and equitable relief, including compensatory damages, restitution, injunctive relief, costs of suit, interest, and such further relief as the Court deems just and proper.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs James Ramirez, Christopher Ellis, and Jalen Delgado respectfully pray that, after trial by jury, the Court enter judgment and against Defendant Apple, Inc. and award full relief under the Consumers Legal Remedies Act, the Louisiana Unfair Trade Practices and Consumer Protection Law, Massachusetts General Laws Chapter 93A, and all other applicable law.

Plaintiffs further pray for an award of compensatory damages in an amount to be determined at trial, including but not limited to reimbursement of all monies, cryptocurrency, and other digital assets wrongfully lost through the fraudulent Sparrow application and related schemes, together with pre-judgment and post-judgment interest as permitted by law.

Plaintiffs pray for treble, multiple, and enhanced damages to the fullest extent allowed by statute, including under Louisiana Revised Statutes title 51, section 1409, Massachusetts General Laws Chapter 93A, section 9, and the California Consumers

Legal Remedies Act, based on Apple's knowing, willful, and bad-faith continuation of unfair and deceptive acts and practices after notice of fraudulent Sparrow-related applications and similar scam cryptocurrency apps on the App Store.

Plaintiffs pray for punitive and exemplary damages sufficient to punish Apple for its fraudulent, reckless, and grossly negligent conduct and to deter similar misconduct in the future, in light of Apple's long-running safety and vetting campaign, its knowledge that the App Store hosted spoofed and fraudulent cryptocurrency applications, and its failure to warn or protect consumers from foreseeable theft of digital assets.

Plaintiffs pray for restitution and disgorgement of all ill-gotten gains, revenues, and benefits Apple obtained as a result of the conduct alleged in this Complaint, including revenues derived from the sale and marketing of Apple devices and services as part of a purportedly "safe and trusted" ecosystem and from distribution of applications through the App Store, to the fullest extent permitted by law.

Plaintiffs further pray for injunctive and equitable relief, including orders requiring Apple to implement, maintain, and publicly disclose reasonable vetting, monitoring, and remedial procedures designed to prevent spoofed, fraudulent, and malicious applications from being approved, ranked, or recommended in the App Store; requiring clear, prominent, and non-misleading warnings and disclosures regarding the limitations of App Store review and the risks associated with cryptocurrency applications; requiring Apple to issue corrective advertising and consumer notices concerning prior misrepresentations about App Store safety and vetting; and prohibiting

Apple from making false or misleading statements about the safety, security, and trustworthiness of applications available through the App Store.

Plaintiffs pray for an award of reasonable attorneys' fees, expenses, and costs of suit pursuant to all applicable statutes, including without limitation Louisiana Revised Statutes title 51, section 1409, Massachusetts General Laws Chapter 93A, section 9, the Consumers Legal Remedies Act, and any other fee-shifting provision or equitable doctrine supporting recovery of fees for the prosecution of this action, together with expert fees and other litigation expenses.

Plaintiffs pray for such additional legal and equitable relief as the Court may deem just, proper, and necessary to fully compensate Plaintiffs for their injuries, to restore them as nearly as possible to the position they occupied before Apple's wrongful conduct, and to prevent and remedy ongoing and future harm resulting from Apple's design, operation, and marketing of the App Store.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand trial by jury on all claims so triable as of right.

Dated: July 24, 2026 Respectfully submitted,

/s/ Kiley Grombacher
Kiley L. Grombacher
Bradley Grombacher, LLP
31355 Oak Crest Drive, Suite 210
Westlake Village, CA 91361
Kgrombacher@bradleygrombacher.com
Telephone: 805-270-7100
Facsimile: 805-270-7589

Aylstock, Witkin, Kreis & Overholtz, PLC
Daniel J. Thornburgh (pro hac vice) Reagan Charleston Thomas (pro hac vice) Kimberly Tanner (pro hac vice)
17 East Main Street, Suite 200
Pensacola, FL 32502
Telephone: 850-202-1010
Fax: 850-916-7449
rthomas@awkolaw.com
dthornburgh@awkolaw.com
ktanner@awkolaw.com

-and-

Daniel J. Thornburgh, Esq. (pro hac vice admission forthcoming)
Reagan Charleston Thomas, Esq. (pro hac vice admission forthcoming)
Kimberly Tanner (pro hac vice admission forthcoming)

Counsel for Plaintiffs