

1 Jason M. Ingber (SBN 318323)
2 **LEVI & KORSINSKY, LLP**
3 3580 Wilshire Boulevard, Suite 1260
4 Los Angeles, California 90010-2513
5 Telephone: (213) 805-8373
6 Email: jingber@zlk.com

7 Mark Reich
8 Michael N. Pollack
9 **LEVI & KORSINSKY, LLP**
10 33 Whitehall Street, 27th Floor
11 New York, NY 10004
12 T: (212) 363-7500
13 F: (212) 363-7171
14 E: mreich@zlk.com
15 E: mpollack@zlk.com

16 **pro hac vice forthcoming*

17 *Counsel for Plaintiff*

18 **UNITED STATES DISTRICT COURT**
19 **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

20 Maria Rosado-Wright, individually and on
21 behalf of all others similarly situated,
22 Plaintiff,
23 v.
24 APPLE INC.,
25 Defendant.

Case No.:

CLASS ACTION COMPLAINT
JURY TRIAL DEMANDED

26 Plaintiff Maria Rosado-Wright (“Plaintiff”), individually and on behalf of all others similarly
27 situated, by and through undersigned counsel, brings this Class Action Complaint against Defendant
28 Apple Inc. (“Apple” or “Defendant”). Plaintiff alleges the following upon information and belief

1 based on the investigation of counsel, except as to those allegations that specifically pertain to
2 Plaintiff, which are alleged upon personal knowledge.

3 NATURE OF THE ACTION

4 1. Apple sells privacy. It advertises privacy as a defining attribute of its products, and
5 it charges for privacy features that it does not include with a free account.¹

6 2. iCloud Private Relay (“Private Relay”) is one of those features. Apple does not offer
7 Private Relay to holders of free iCloud accounts. Apple offers it only to consumers who pay for a
8 subscription to iCloud+, which Apple sells at prices ranging from \$0.99 to \$59.99 per month.²

9 3. Apple represents that Private Relay solves a specific problem. Apple states that
10 when a consumer browses the web, the consumer's DNS records and IP address, can be seen by your
11 network provider and the websites you visit, and that this information “could be used to determine
12 your identity and build a profile of your location and browsing history over time.”³

13 4. Apple represents that Private Relay prevents that result. Apple states that Private
14 Relay “is designed to protect your privacy by ensuring that when you browse the web in Safari, no
15 single party” can “see both who you are and what sites you're visiting.”⁴ Apple identifies itself as
16 one of the parties that cannot: “not even Apple.”

17 5. Apple represents that Private Relay achieves this through two relays operated by
18 different entities. Apple states that a consumer's requests “are sent through two separate, secure
19 internet relays,” that the first relay “is operated by Apple” and sees the consumer's IP address but
20 not the destination, and that the second relay “is operated by a third-party content provider” and
21 “generates a temporary IP address” before connecting the consumer to the site.⁵

22 ¹ Privacy, APPLE, <https://www.apple.com/privacy/> (last visited Aug. 13, 2026).

23 ² iCloud+, APPLE, <https://www.apple.com/icloud/> (last visited Aug. 13, 2026).

24 ³ About iCloud Private Relay, APPLE SUPPORT, <https://support.apple.com/en-us/102602> (last visited Aug. 13, 2026).

25 ⁴ *Id.*

26 ⁵ *Id.*

1 6. Those representations were false. On August 4, 2026, security researchers Talal Haj
2 Bakry and Tommy Mysk published findings identifying three features of WebKit, the browser
3 engine Apple builds and requires every browser on iOS to use, that send network requests outside
4 the path Private Relay proxies. Each one delivers the consumer's real IP address or DNS queries to
5 the remote server while Private Relay is turned on.⁶

6 7. The three features are DNS prefetching, WebAuthn Related Origin Requests, and
7 WebTransport. The researchers state that each “bypass the configured proxy and send traffic directly
8 from the device, which exposes the user's real network,” and that “[t]he same leaks also affect
9 Apple's iCloud Private Relay.”⁷

10 8. The WebAuthn path requires nothing of the consumer. When a web page requests
11 a passkey associated with another domain, the operating system's credential service issues the
12 request itself rather than routing it through Safari, and the destination server receives the device's
13 real IP address. The request fires whether or not the consumer has a passkey saved for that site, and
14 iOS displays no prompt.⁸

15 9. The leaks are not theoretical. The researchers published a proof-of-concept site that
16 demonstrates them, and 404 Media, which first reported the findings, verified that a test site could
17 read a protected user's real IP address.⁹

18
19
20
21 ⁶ Talal Haj Bakry & Tommy Mysk, *IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple*
22 *iCloud Private Relay*, MYSK BLOG, [https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/)
23 [ip-leak/](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/) (last visited Aug. 13, 2026).

24 ⁷ *Id.*

25 ⁸ *Id.*

26 ⁹ *Apple's 'Private Relay' Is Exposing Users' Real IP Addresses*, 404 MEDIA,
27 <https://www.404media.co/apples-private-relay-is-exposing-users-real-ip-addresses/> (last visited Aug.
28 13, 2026).

1 10. Apple has acknowledged the defect. Within a day of publication, Apple updated the
2 status of the researchers' report in its security program to state that Apple was “planning to address
3 the issue you reported,” and identified a fix for fall 2026.¹⁰

4 11. Apple has not refunded any part of the subscription price it charged for a privacy
5 feature that did not deliver the represented protection, and it continues to sell iCloud+ on the same
6 representations.

7 12. Plaintiff and the members of the proposed Class paid Apple for a feature that did
8 not do what Apple said it did. Had they known that WebKit would deliver their real IP addresses to
9 the sites they visited while Private Relay was enabled, they would not have subscribed to iCloud+,
10 or would have paid less for it. Because the feature did not work as represented, subscribers overpaid:
11 the price reflected a protection Apple promised but did not provide.

12 13. Plaintiff brings this action on behalf of a nationwide class of iCloud+ subscribers
13 who enabled Private Relay, and a Florida subclass, for violations of California's Unfair Competition
14 Law, False Advertising Law, and Consumers Legal Remedies Act, and for fraud, negligent
15 misrepresentation, breach of contract, and unjust enrichment.

16
17
18 **PARTIES**

19 14. Plaintiff Maria Rosado-Wright is a natural person and a citizen of the State of
20 Florida. Plaintiff pays \$2.99 each month for iCloud+. Plaintiff relied on the Apple statements about
21 privacy and security when she was availing the subscription with iCloud.

22
23
24 ¹⁰ Chance Miller, *iCloud Private Relay might be leaking your real IP address, researchers say*,
25 9TO5MAC, <https://9to5mac.com/2026/08/05/icloud-private-relay-leaking-your-ip-address/> (last visited
26 Aug. 13, 2026).

15. Defendant Apple Inc. is a California corporation with its principal place of business at One Apple Park Way, Cupertino, California 95014, in Santa Clara County. Apple designs, markets, and sells the iCloud+ subscription and the Private Relay feature at issue, and develops WebKit.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because the proposed Class contains more than 100 members, at least one member of the proposed Class is a citizen of a state different from Apple, and the aggregate amount in controversy exceeds \$5,000,000, exclusive of interest and costs.

17. This Court has personal jurisdiction over Apple because Apple is incorporated in California, maintains its principal place of business in this District, and conducts substantial business throughout this District.

18. Venue is proper in this District under 28 U.S.C. § 1391(b) because Apple resides in this District and because a substantial part of the events giving rise to the claims occurred here.

19. Venue is also proper because Apple's own iCloud Terms and Conditions provide that the subscriber and Apple “agree to submit to the personal and exclusive jurisdiction of the courts located within the county of Santa Clara, California, to resolve any dispute or claim arising from this Agreement.”¹¹

20. Assignment to the San Jose Division is proper under Civil Local Rule 3-2(c) and (e) because Apple resides in Santa Clara County and a substantial part of the events giving rise to the claims occurred in Santa Clara County.

¹¹ *iCloud Terms & Conditions*, APPLE, <https://www.apple.com/legal/internet-services/icloud/en/terms.html> (last visited Aug. 13, 2026).

CHOICE OF LAW

21. Apple's iCloud Terms and Conditions provide that “this Agreement and the relationship between you and Apple shall be governed by the laws of the State of California, excluding its conflicts of law provisions.”¹²

22. Apple drafted that provision, applies it to subscribers nationwide, and requires assent to it as a condition of subscribing to iCloud+. California law therefore governs the claims of the Nationwide Class.

23. California also has a significant interest in applying its consumer protection statutes to this conduct. Apple is headquartered in California, the representations at issue were developed and disseminated from California, and the decisions concerning Private Relay and WebKit were made in California.

FACTUAL ALLEGATIONS

A. Apple Sells Privacy as a Product Feature

24. Apple markets privacy as a reason to buy and keep Apple products. Apple publishes a dedicated privacy section of its website and describes privacy as a fundamental right.¹³

25. Apple's privacy marketing is not limited to general statements. Apple identifies specific features, describes what each is designed to prevent, and distinguishes the protection those features provide from what a consumer would otherwise experience.

26. These representations matter to consumers, and Apple knows it: Apple has built privacy into the center of its advertising precisely because privacy sells.

¹² *Id.*

¹³ *Privacy*, APPLE, <https://www.apple.com/privacy/> (last visited Aug. 13, 2026).

B. Apple Sells Private Relay Only to Paying iCloud+ Subscribers

27. Apple provides every Apple account holder with 5GB of free iCloud storage. Apple sells additional storage, together with a set of features it labels privacy features, under the name iCloud+. ¹⁴

28. Apple prices iCloud+ in tiers. Apple's website advertises tiers at \$0.99 per month for 50GB, \$2.99 per month for 200GB, and \$9.99 per month for 2TB, and Apple offers higher tiers at prices up to \$59.99 per month. ¹⁵

29. Apple states on the same page that “[e]very iCloud+ plan includes Apple Invites, iCloud Private Relay, Hide My Email, Custom Email Domain, and HomeKit Secure Video.” ¹⁶ Private Relay is the second feature Apple names.

30. Apple's plan comparison identifies Private Relay as not included with a free iCloud account and included with every paid iCloud+ tier. A consumer who wants Private Relay must pay for it. ¹⁷

¹⁴ *iCloud+*, APPLE, <https://www.apple.com/icloud/> (last visited Aug. 13, 2026).

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

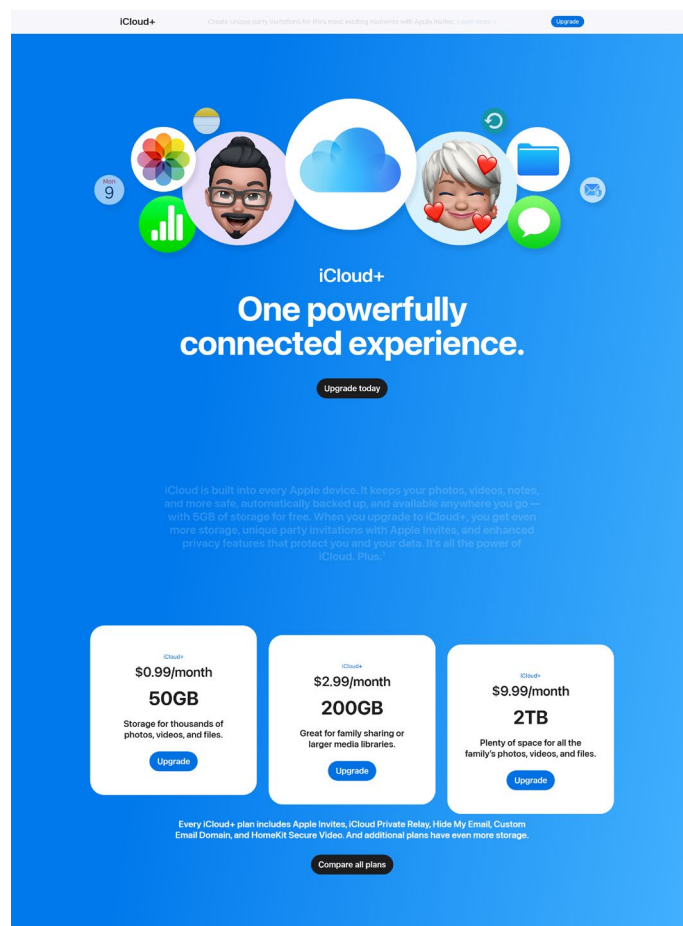


Figure 1 – Apple's iCloud+ page, showing the subscription tiers and Apple's statement that every iCloud+ plan includes iCloud Private Relay.

31. Apple introduced Private Relay as part of iCloud+ in 2021 and released it to the public with iOS 15 in September 2021.

32. Apple has sold iCloud+ subscriptions on the strength of Private Relay continuously since that time.

C. Apple Represents That No Party, Including Apple, Can Link a Subscriber's Identity to the Sites the Subscriber Visits

33. Apple publishes a support page titled “About iCloud Private Relay.”¹⁸ The page states that Private Relay is “part of an iCloud+ subscription” and “helps protect your privacy when you browse the web in Safari.”¹⁹

34. The page describes the problem Private Relay is sold to solve. It states that in ordinary browsing, information in a consumer's web traffic, “such as your DNS records and IP address, can be seen by your network provider and the websites you visit,” and that this information “could be used to determine your identity and build a profile of your location and browsing history over time.”²⁰

35. The page then makes the representation at the center of this case. It states that Private Relay “is designed to protect your privacy by ensuring that when you browse the web in Safari, no single party” can “see both who you are and what sites you're visiting.”²¹ Apple names itself as one of the parties so barred, stating “not even Apple.”

36. The page describes the mechanism. It states that “[w]hen Private Relay is enabled, your requests are sent through two separate, secure internet relays”; that the consumer's “IP address is visible to your network provider and to the first relay, which is operated by Apple,” while the consumer's “DNS records are encrypted, so neither party can see the address of the website you're trying to visit”; and that “[t]he second relay, which is operated by a third-party content provider, generates a temporary IP address, decrypts the name of the website you requested, and connects you

¹⁸ *About iCloud Private Relay*, APPLE SUPPORT, <https://support.apple.com/en-us/102602> (last visited Aug. 13, 2026).

¹⁹ *Id.*

²⁰ *Id.*

²¹ *Id.*

to the site.”²² Under the design Apple describes, the website a subscriber visits never receives the subscriber's real IP address.

About iCloud Private Relay

iCloud Private Relay — part of an iCloud+ subscription — helps protect your privacy when you browse the web in Safari.

How Private Relay works

Normally when you browse the web, information contained in your web traffic, such as your DNS records and IP address, can be seen by your network provider and the websites you visit. This information could be used to determine your identity and build a profile of your location and browsing history over time.

iCloud Private Relay is designed to protect your privacy by ensuring that when you browse the web in Safari, no single party — not even Apple — can see both who you are and what sites you're visiting.

When Private Relay is enabled, your requests are sent through two separate, secure internet relays.

- Your IP address is visible to your network provider and to the first relay, which is operated by Apple. Your DNS records are encrypted, so neither party can see the address of the website you're trying to visit.
- The second relay, which is operated by a third-party content provider, generates a temporary IP address, decrypts the name of the website you requested, and connects you to the site.



All of this is done using the latest internet standards to maintain a high-performance browsing experience while protecting your privacy.

[Set up iCloud Private Relay on all of your devices](#)

[Manage Private Relay for specific websites, networks, or system settings](#)

iCloud Private Relay is not available in all countries or regions. Without access to your IP address, some websites may require extra steps to sign in or access content.

Private Relay and network speed tests

Private Relay uses a single, secure connection to maintain privacy and performance. This design may impact how throughput is reflected in network speed tests that typically open several simultaneous connections to deliver the highest possible result. While some speed test measurements may appear lower when Private Relay is enabled, your actual browsing experience remains fast and private.

Additional resources for developers and network administrators

If you're a website owner or developer, network administrator, or app developer, learn how to [provide the best possible experience for users of Private Relay on your network](#).

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. [Contact the vendor](#) for additional information.

Published Date: August 31, 2023

Figure 2 – Apple's support page “About iCloud Private Relay,” describing the two-relay design and stating that no single party can see both who the subscriber is and what sites the subscriber is visiting.

37. Apple published that page on August 31, 2023, and it remained on Apple's website in that form as of the filing of this Complaint.²³

38. Apple's representations are unqualified as to the outcome. Apple discloses that Private Relay is unavailable in some countries and that some websites may require extra steps to

²² *Id.*

²³ *Id.*

1 sign in without access to an IP address. Apple does not disclose that features of Apple's own browser
2 engine send the consumer's real IP address to the visited site while Private Relay is enabled.²⁴

3 **D. Three WebKit Features Send the Subscriber's Real IP Address and DNS Queries**
4 **Outside Private Relay**

5 39. WebKit is the browser engine Apple develops and uses in Safari. Apple's App Store
6 policy requires every browser on iOS to use WebKit, so a subscriber cannot avoid the behavior
described below by using a different iOS browser.²⁵

7 40. On August 4, 2026, Talal Haj Bakry and Tommy Mysk published "IP and DNS
8 Leaks in WebKit Affecting Proxy Browsers and Apple iCloud Private Relay."²⁶ They identified
9 three WebKit features that "bypass the configured proxy and send traffic directly from the device,
10 which exposes the user's real network," and stated that "[t]he same leaks also affect Apple's iCloud
11 Private Relay."²⁷ None of the three features is unusual. Each is a standard part of the modern web
12 that ordinary websites use, so a subscriber encounters them in the course of ordinary browsing.
13
14
15
16
17
18
19
20
21

22 ²⁴ *Id.*

23 ²⁵ *Talal Haj Bakry & Tommy Mysk, IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple*
24 *iCloud Private Relay*, MYSK BLOG, [https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/)
[ip-leak/](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/) (last visited Aug. 13, 2026).

25 ²⁶ *Id.*

26 ²⁷ *Id.*

MYSK BLOG

[Apps](#) [Home](#) [Psylo](#) [X](#) [Mastodon](#) [YouTube](#) [Buy me a coffee](#)

IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple iCloud Private Relay

2026-08-04 :: by [Talal Haj Bakry](#) and [Tommy Mysk](#)

WebKit-based browsers on iOS and macOS can be configured to route all web traffic through proxy servers, which is how Tor browsers on iOS and our own Psylo work. We found three WebKit features – DNS prefetching, WebAuthn Related Origin Requests, and WebTransport – that bypass the configured proxy and send traffic directly from the device, which exposes the user's real network. The same leaks also affect Apple's iCloud Private Relay. All three are fixed in Psylo 1.3.1.

Table of Contents

- [Summary](#)
- [Background](#)
 - [Proxy Configuration on iOS and macOS](#)
 - [DNS Leak Reported by a Psylo User](#)
 - [iCloud Private Relay](#)
- [1. DNS Prefetching](#)
- [2. WebAuthn Related Origin Requests](#)
- [3. WebTransport](#)
- [Mitigations Introduced in Psylo 1.3.1](#)

Figure 3 – The August 4, 2026 research publication identifying the three WebKit features that bypass iCloud Private Relay.

a. DNS Prefetching

41. A web page can instruct the browser to resolve a hostname in advance using a DNS prefetch hint. The researchers found that WebKit “resolves the hostname through the device's normal DNS path, regardless of any proxy set by the browser.”²⁸

42. The consequence is that a page can embed unique hostnames and observe the resulting queries arriving from the visitor's actual network. The researchers state that the query “reaches the authoritative server from the device's real network even with Private Relay enabled.”²⁹

²⁸ *Id.*

²⁹ *Id.*

43. The researchers identify this behavior as present beginning with iOS 26.0, released in September 2025.³⁰

b. WebAuthn Related Origin Requests

44. A website uses a WebAuthn Related Origin Request to validate that a passkey created for one domain may be used on another. The researchers found that WebKit “hands WebAuthn ceremonies to the operating system's credential service, which issues the HTTPS request itself, directly from the device and unaware of any proxy.”³¹

45. Because the request originates with the operating system rather than with Safari, it never enters the proxied path. The researchers state that “[t]he destination server sees the device's real IP address.”³²

46. A website can trigger the request without any action by the consumer and without the consumer having saved a passkey for that site. The researchers describe the request firing with no user interaction and no interface ever appearing.³³

47. Any site that supports passkeys, or that presents itself as supporting passkeys, can therefore obtain the real IP address of a subscriber who has Private Relay enabled.³⁴

48. The researchers identify this behavior as present beginning with iOS 18.0, released in September 2024, approximately three years after Apple began sale of Private Relay.³⁵

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

³³ *Id.*

³⁴ *Apple's 'Private Relay' Is Exposing Users' Real IP Addresses*, 404 MEDIA, <https://www.404media.co/apples-private-relay-is-exposing-users-real-ip-addresses/> (last visited Aug. 13, 2026).

³⁵ *Talal Haj Bakry & Tommy Mysk, IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple iCloud Private Relay*, MYSK BLOG, <https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/> (last visited Aug. 13, 2026).

1 *c. WebTransport*

2 49. WebTransport allows a page to open a connection over HTTP/3. The researchers
3 found that calling the WebTransport constructor “opens a QUIC connection straight from the
4 device,” and that WebKit “builds the connection with its own network parameters and never offers
5 it the session's proxy.”³⁶

6 50. The result is the same. The researchers state that the receiving “server sees the
7 device's real IP address instead of the proxy's,” and that this occurs “even with Private Relay
8 enabled.”³⁷

9 51. The researchers identify this behavior as present beginning with iOS 26.4, released
10 in March 2026.³⁸

11 **E. Independent Testing Confirmed the Leaks**

12 52. The researchers published a proof-of-concept website that allows any user to test
13 whether the described leaks occur on that user's own device.³⁹

14 53. 404 Media, which first reported the findings, verified that a test site could read a
15 protected user's real IP address.⁴⁰ The leaks are therefore reproducible on demand and occur under
16 ordinary conditions.

17 54. TechCrunch separately published a consumer advisory reporting that Apple's
18 Private Relay can leak a subscriber's real IP address.⁴¹

20 ³⁶ *Id.*

21 ³⁷ *Id.*

22 ³⁸ *Id.*

23 ³⁹ *Id.*

24 ⁴⁰ *Apple's 'Private Relay' Is Exposing Users' Real IP Addresses*, 404 MEDIA,
25 <https://www.404media.co/apples-private-relay-is-exposing-users-real-ip-addresses/> (last visited Aug.
26 13, 2026).

27 ⁴¹ *PSA: Apple's Private Relay can leak your real IP address*, TECHCRUNCH,
28 <https://techcrunch.com/2026/08/05/psa-apples-private-relay-can-leak-your-real-ip-address/> (last
visited Aug. 13, 2026).

F. Apple Acknowledged the Defect

55. The researchers reported the issue to Apple through Apple's security reporting program.⁴²

56. Within a day of publication, the status of that report changed to state that Apple was “planning to address the issue you reported.”⁴³ Apple identified a fix for fall 2026.

57. Apple knew or should have known that the protection had failed. Yet it left its representations in place, kept subscribers in the dark, and offered neither refund nor price adjustment.

G. An Exposed IP Address Is the Harm Private Relay Was Sold to Prevent

58. An IP address identifies the network a device is using and can be used to approximate the user's location. Apple says so itself, stating that DNS records and IP addresses “could be used to determine your identity and build a profile of your location and browsing history over time.”⁴⁴

59. That is the precise capability Apple represented Private Relay would deny to the websites a subscriber visits. A subscriber who enabled Private Relay and visited a site that used any of the three WebKit features .was left worse off than Apple's own description of unprotected browsing: the very site the subscriber visited received the real IP address Private Relay was sold to conceal the subscriber's real IP address, and the subscriber had been told that it could not.

⁴² Talal Haj Bakry & Tommy Mysk, *IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple iCloud Private Relay*, MYSK BLOG, <https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/> (last visited Aug. 13, 2026).

⁴³ Chance Miller, *iCloud Private Relay might be leaking your real IP address, researchers say*, 9TO5MAC, <https://9to5mac.com/2026/08/05/icloud-private-relay-leaking-your-ip-address/> (last visited Aug. 13, 2026).

⁴⁴ *About iCloud Private Relay*, APPLE SUPPORT, <https://support.apple.com/en-us/102602> (last visited Aug. 13, 2026).

60. The exposure is silent. Nothing in Safari or in the Private Relay settings indicates to a subscriber that a given page has obtained the subscriber's real IP address, and the WebAuthn path produces no prompt at all.⁴⁵ A subscriber could not detect the exposure and could not prevent it.

H. Plaintiff's Experience

61. Plaintiff relied on and understood Apple's privacy representations to mean that the websites Plaintiff visited in Safari would not receive Plaintiff's real IP address. That understanding was material to Plaintiff's decision to subscribe to iCloud+ and to continue paying for it.

62. Plaintiff did not know, and had no reasonable way to learn, that features of WebKit sent Plaintiff's real IP address and DNS queries outside Private Relay.

63. Had Apple disclosed that WebKit would deliver Plaintiff's real IP address to the sites Plaintiff visited while Private Relay was enabled, Plaintiff would not have subscribed to iCloud+, or would not have paid the price Plaintiff paid. Plaintiff's reliance was reasonable: the conduct Apple concealed was invisible to any ordinary user of Safari, and nothing available to Plaintiff contradicted Apple's representations.

I. Class Members Paid for a Protection They Did Not Receive

64. Apple charged a subscription price for iCloud+ that included Private Relay as an advertised feature. Because the feature did not work as represented, subscribers overpaid: the price reflected a protection Apple promised but did not provide.

65. Plaintiff and the members of the Class did not receive the benefit of their bargain. They paid for a subscription whose advertised privacy protection did not function as Apple stated, and they would have paid less, or nothing, had the truth been disclosed. The gap between the price

⁴⁵ Talal Haj Bakry & Tommy Mysk, *IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple iCloud Private Relay*, MYSK BLOG, <https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/> (last visited Aug. 13, 2026).

Apple charged and the value of what Apple delivered is common to every member of the Class and measurable by common proof.

TOLLING

66. To the extent Apple contends that any claim accrued before subscribers could have learned of the conduct alleged, that contention would fail. Any applicable statute of limitations was tolled by the discovery rule. The behavior of WebKit described above is not observable by a consumer using Safari, and it was not publicly identified until August 4, 2026.⁴⁶

67. Any applicable statute of limitations was tolled by Apple's concealment. Apple controls WebKit and Private Relay, and Apple did not disclose that WebKit sent subscribers' real IP addresses and DNS queries outside Private Relay while continuing to represent that no single party could link a subscriber's identity to the sites the subscriber visited.

68. Apple is estopped from asserting any statute of limitations defense. Apple possessed the information necessary to disclose the conduct, made representations inconsistent with it, and left those representations in place after acknowledging the defect.

CLASS ACTION ALLEGATIONS

69. Plaintiff brings this action individually and on behalf of the following Nationwide Class and Subclass:

Nationwide Class: All persons in the United States who, during the Class Period, paid for an iCloud+ subscription and enabled iCloud Private Relay (the "Nationwide Class").

Florida Subclass: All persons who, while residing in the State of Florida during the Class Period, paid for an iCloud+ subscription and enabled iCloud Private Relay (the "Florida Subclass").

70. The "Class Period" means the period from the public release of iCloud Private Relay in September 2021 through the date of judgment in this action.

⁴⁶ *Id.*

1 71. Excluded from the Class and Subclass are Apple, its officers, directors, agents,
2 employees, subsidiaries, and affiliates; counsel for Plaintiff and counsel for Apple; the judicial
3 officers to whom this action is assigned and members of their immediate families; and any person
4 who timely and validly requests exclusion.

5 72. Plaintiff reserves the right to amend the Class and Subclass definitions if further
6 investigation or discovery reveals that they should be expanded, narrowed, divided into additional
7 subclasses, or otherwise modified.

8 73. Numerosity (Rule 23(a)(1)): The Class and Subclass are so numerous that joinder
9 of all members is impracticable. Apple sells iCloud+ subscriptions to consumers throughout the
10 United States, and Private Relay is included with every paid tier. The precise size of the Class and
11 Subclass is presently unknown to Plaintiff but is readily ascertainable from Apple's subscription and
12 account records.

13 74. Commonality and Predominance (Rules 23(a)(2) and 23(b)(3)): Common questions
14 of law and fact predominate over questions affecting only individual members. Those questions
15 include:

- 16 a. Whether Apple represented that Private Relay prevents any single party from linking a
17 subscriber's identity to the sites the subscriber visits;
- 18 b. Whether the WebKit features described above sent subscribers' real IP addresses or DNS
19 queries outside Private Relay;
- 20 c. Whether Apple's representations concerning Private Relay were false or misleading to a
21 reasonable consumer;
- 22 d. Whether Apple omitted material facts concerning Private Relay that it had a duty to
23 disclose;
- 24 e. Whether Apple knew or should have known that its representations were false or
25 misleading;

- f. Whether Apple's conduct violated the Unfair Competition Law, the False Advertising Law, or the Consumers Legal Remedies Act;
- g. Whether Apple was unjustly enriched by the subscription revenue it retained; and
- h. The appropriate measure of damages, restitution, and injunctive relief.

75. Typicality (Rule 23(a)(3)): Plaintiff's claims are typical of the claims of the Class and Subclass. Plaintiff paid for iCloud+, enabled Private Relay, and was exposed to the same representations Apple made to every other member.

76. Adequacy (Rule 23(a)(4)): Plaintiff will fairly and adequately protect the interests of the Class and Subclass. Plaintiff has no interests antagonistic to those of the Class and Subclass and has retained counsel experienced in consumer class action litigation.

77. Superiority (Rule 23(b)(3)): A class action is superior to other available methods for the fair and efficient adjudication of this controversy. The monetary loss to each individual subscriber is small relative to the cost of individual litigation, and absent a class action most members would have no practical means of redress.

78. Ascertainability: Members of the Class and Subclass are identifiable from Apple's own records, which reflect who purchased an iCloud+ subscription, during what period, at what price, and which accounts had Private Relay enabled.

79. Injunctive and Declaratory Relief (Rule 23(b)(2)): Apple has acted on grounds generally applicable to the Class and Subclass, making final injunctive and declaratory relief appropriate as to the Class and Subclass as a whole.

CAUSES OF ACTION

COUNT I

VIOLATIONS OF THE CALIFORNIA UNFAIR COMPETITION LAW

Cal. Bus. & Prof. Code § 17200, et seq.

(On Behalf of the Nationwide Class)

80. Plaintiff incorporates the allegations in paragraphs 1 through 79 by reference as if fully set forth herein.

81. California Business and Professions Code sections 17200, et seq. (the “UCL”) prohibits unfair competition and provides that unfair competition “shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising.”⁴⁷

a. The Unlawful Prong

82. Apple's conduct is unlawful because it violates the False Advertising Law, Cal. Bus. & Prof. Code sections 17500, et seq., and the Consumers Legal Remedies Act, Cal. Civ. Code sections 1750, et seq., as alleged in Counts II and III.

83. Apple's conduct is also unlawful because it constitutes deceit under California Civil Code sections 1709 and 1710, which impose liability for the suppression of a fact by one bound to disclose it and for the assertion of a fact not warranted by the information the speaker possesses.

b. The Fraudulent Prong

84. Apple's conduct is fraudulent because Apple's representations concerning Private Relay were likely to deceive a reasonable consumer. A reasonable consumer reading that no single party can *see* both who the consumer is and what sites the consumer visits would understand that the sites visited do not receive the consumer's real IP address.

⁴⁷ Cal. Bus. & Prof. Code § 17200.

1 85. Apple's omissions were likewise likely to deceive. Apple disclosed limitations of
2 Private Relay that it considered material, including geographic availability and sign-in friction, while
3 omitting that features of Apple's own browser engine defeated the protection entirely.

4 *c. The Unfair Prong*

5 86. Apple's conduct is unfair. Charging a subscription price for a privacy feature while
6 failing to disclose that the feature does not deliver the represented protection offends established
7 public policy and is immoral, unethical, oppressive, and unscrupulous.

8 87. The harm to consumers is substantial, is not outweighed by any countervailing
9 benefit to consumers or to competition, and is not reasonably avoidable by consumers, who cannot
10 observe the conduct and are given no notice of it.

11 88. Plaintiff and the members of the Class lost money or property as a result of Apple's
12 conduct. They paid subscription fees they would not have paid, or would have paid in a lesser
13 amount, absent Apple's representations and omissions.

14 89. Plaintiff seeks restitution, disgorgement of amounts Apple unjustly retained, and
15 injunctive relief under Cal. Bus. & Prof. Code section 17203, together with attorneys' fees and costs
16 under Cal. Code Civ. Proc. section 1021.5.

17 **COUNT II**
VIOLATIONS OF THE CALIFORNIA FALSE ADVERTISING LAW
18 **Cal. Bus. & Prof. Code § 17500, et seq.**
19 ***(On Behalf of the Nationwide Class)***

20 90. Plaintiff incorporates the allegations in paragraphs 1 through 79 by reference as if
21 fully set forth herein.

22 91. California Business and Professions Code sections 17500, et seq. (the "FAL")
23 prohibits any statement concerning property or services, disseminated to induce the public to enter
24
25
26

1 into an obligation, that is “untrue or misleading, and which is known, or which by the exercise of
2 reasonable care should be known, to be untrue or misleading.”⁴⁸

3 92. Apple disseminated the representations concerning Private Relay described above
4 through its website and its support documentation, in California and throughout the United States,
5 to induce consumers to purchase iCloud+ subscriptions.

6 93. Those representations were untrue or misleading. Private Relay did not prevent the
7 sites a subscriber visited from obtaining the subscriber's real IP address.

8 94. Apple knew or by the exercise of reasonable care should have known that the
9 representations were untrue or misleading. Apple designs and maintains both WebKit and Private
10 Relay, and the behavior of each is within Apple's knowledge and control.

11 95. Plaintiff and the members of the Class suffered injury in fact and lost money or
12 property as a result, and seek restitution and injunctive relief.

13 **COUNT III**
14 **VIOLATIONS OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT**
15 **Cal. Civ. Code § 1750, et seq.**
16 ***(On Behalf of the Nationwide Class)***

17 96. Plaintiff incorporates the allegations in paragraphs 1 through 79 by reference as if
18 fully set forth herein.

19 97. The Consumers Legal Remedies Act (the “CLRA”) applies to Apple's conduct. An
20 iCloud+ subscription is a service purchased by consumers for personal, family, or household
21 purposes, and Apple's sale of that subscription is a transaction within the meaning of Cal. Civ. Code
22 section 1761.

23 98. Apple violated Cal. Civ. Code section 1770(a)(5) by representing that iCloud+ has
24 characteristics and benefits that it does not have.

25 ⁴⁸ Cal. Bus. & Prof. Code § 17500.
26

100. Apple violated Cal. Civ. Code section 1770(a)(9) by advertising iCloud+ with the intent not to sell it as advertised.

101. Apple's omissions are actionable because Apple had exclusive knowledge of material facts not known to consumers, actively concealed those facts, and made partial representations concerning the limits of Private Relay while suppressing the material fact that its own browser engine defeated the feature.

9 102. Plaintiff seeks injunctive relief under Cal. Civ. Code section 1780(a)(2). Plaintiff is
0 concurrently serving notice on Apple under Cal. Civ. Code section 1782(a) and, if Apple fails to
1 provide an appropriate correction within thirty days, will amend this Complaint to seek damages
2 under the CLRA.

3 103. Plaintiff sent a CLRA letter via certified mail, return receipt requested, on August
4 14, 2026

(On Behalf of the Nationwide Class)

7 104. Plaintiff incorporates the allegations in paragraphs 1 through 79 by reference as if
8 fully set forth herein.

105. **WHO.** Apple Inc. made each of the representations alleged herein. Apple authored them, published them, controlled their content, and alone possessed the ability to correct or withdraw them. Apple disseminated them from its headquarters at One Apple Park Way, Cupertino, California, through channels Apple owns and operates, to Plaintiff and to every consumer to whom it sold an iCloud+ subscription.

106. **WHAT.** Apple represented that iCloud Private Relay "is designed to protect your privacy by ensuring that when you browse the web in Safari, no single party" can "see both who you

are and what sites you're visiting," including Apple itself — "not even Apple"⁴⁹; that a subscriber's requests "are sent through two separate, secure internet relays," the first "operated by Apple" and the second "operated by a third-party content provider," which "generates a temporary IP address, decrypts the name of the website you requested, and connects you to the site"⁵⁰; that a subscriber's "DNS records are encrypted, so neither party can see the address of the website you're trying to visit"⁵¹; and that "[e]very iCloud+ plan includes Apple Invites, iCloud Private Relay, Hide My Email, Custom Email Domain, and HomeKit Secure Video." ⁵² Each representation conveyed a single message: that a website a subscriber visits in Safari does not receive the subscriber's real IP address while Private Relay is enabled.

107. **WHERE.** Apple made these representations on the pages where it sells iCloud+ subscriptions and on Apple's support page titled "About iCloud Private Relay," published at support.apple.com/en-us/102602.

108. **WHEN.** Apple published the "About iCloud Private Relay" support page on August 31, 2023, and that page remained on Apple's website in the form quoted above continuously through the filing of this Complaint. Apple sold iCloud+ subscriptions on the strength of Private Relay continuously from the feature's public release in September 2021 through the filing of this Complaint.

109. **HOW THE REPRESENTATIONS WERE FALSE.** The representations were false when made and remained false throughout the period alleged. Three features of WebKit — the browser engine Apple develops — bypass the path Private Relay proxies and deliver the subscriber's real IP address or DNS queries directly to the remote server while Private Relay is enabled: DNS

⁴⁹ *About iCloud Private Relay*, APPLE SUPPORT, <https://support.apple.com/en-us/102602> (last visited Aug. 13, 2026).

⁵⁰ *About iCloud Private Relay*, APPLE SUPPORT, <https://support.apple.com/en-us/102602> (last visited Aug. 13, 2026).

⁵¹ *About iCloud Private Relay*, APPLE SUPPORT, <https://support.apple.com/en-us/102602> (last visited Aug. 13, 2026).

⁵² *iCloud+*, APPLE, <https://www.apple.com/icloud/> (last visited Aug. 13, 2026).

1 prefetching, which "resolves the hostname through the device's normal DNS path, regardless of any
 2 proxy set by the browser,"⁵³ present beginning with iOS 26.0 in September 2025; WebAuthn Related
 3 Origin Requests, which WebKit "hands . . . to the operating system's credential service, which issues
 4 the HTTPS request itself, directly from the device and unaware of any proxy,"⁵⁴ so that "[t]he
 5 destination server sees the device's real IP address,"⁵⁵ present beginning with iOS 18.0 in September
 6 2024, and firing with no user interaction, no saved passkey, and no interface; and WebTransport, which
 7 "opens a QUIC connection straight from the device," so that the receiving "server sees the device's
 8 real IP address instead of the proxy's,"⁵⁶ present beginning with iOS 26.4 in March 2026. Each feature
 9 is a standard component of the modern web that ordinary websites use, so a subscriber encountered
 10 them in the course of ordinary browsing.

11 110. Apple concealed and failed to disclose that features of WebKit sent subscribers' real
 12 IP addresses and DNS queries outside Private Relay. Apple had a duty to disclose that fact because
 13 Apple had exclusive knowledge of it, because Apple actively concealed it, and because Apple made
 14 partial representations concerning the limits of Private Relay that were misleading without it.

15 111. Apple knew the representations were false, or made them recklessly and without
 16 regard for their truth. Apple develops WebKit, controls its release, and determines what network
 17 requests it makes.

18
 19 ⁵³ Talal Haj Bakry & Tommy Mysk, *IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple*
 20 *iCloud Private Relay*, MYSK BLOG, [https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/)
 21 [ip-leak/](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/) (last visited Aug. 13, 2026).

22 ⁵⁴ Talal Haj Bakry & Tommy Mysk, *IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple*
 23 *iCloud Private Relay*, MYSK BLOG, [https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/)
 24 [ip-leak/](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/) (last visited Aug. 13, 2026).

25 ⁵⁵ Talal Haj Bakry & Tommy Mysk, *IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple*
 26 *iCloud Private Relay*, MYSK BLOG, [https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/)
 27 [ip-leak/](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/) (last visited Aug. 13, 2026).

28 ⁵⁶ Talal Haj Bakry & Tommy Mysk, *IP and DNS Leaks in WebKit Affecting Proxy Browsers and Apple*
iCloud Private Relay, MYSK BLOG, [https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/)
[ip-leak/](https://mysk.blog/2026/08/04/webkit-proxy-icloud-private-relay-ip-leak/) (last visited Aug. 13, 2026).

112. Apple intended that consumers rely on the representations. Apple made them on the pages where it sells iCloud+ and on the support page describing the feature, for the purpose of inducing subscriptions.

113. Plaintiff and the members of the Class reasonably relied on the representations. The conduct concealed was not observable, and consumers had no means of discovering it.

114. Plaintiff and the members of the Class were damaged in the amount of the subscription fees they paid, or the difference between what they paid and the value of what they received.

115. Apple's conduct was willful and in conscious disregard of the rights of consumers, warranting punitive damages under Cal. Civ. Code section 3294.

COUNT V
NEGLIGENT MISREPRESENTATION
(On Behalf of the Nationwide Class)

116. Plaintiff incorporates the allegations in paragraphs 1 through 79 by reference as if fully set forth herein.

117. Apple made the representations concerning Private Relay described above without reasonable grounds for believing them to be true.

118. Apple owed a duty to consumers to exercise reasonable care in describing the protection Private Relay provided, because Apple charged for that protection and possessed the sole means of verifying it.

119. Apple breached that duty. Apple represented an outcome that its own browser engine prevented from occurring.

120. Plaintiff and the members of the Class justifiably relied on the representations and were damaged as a result.

COUNT VI
**BREACH OF CONTRACT AND OF THE IMPLIED COVENANT OF GOOD FAITH AND
FAIR DEALING**
(On Behalf of the Nationwide Class)

121. Plaintiff incorporates the allegations in paragraphs 1 through 79 by reference as if fully set forth herein.

122. Plaintiff and each member of the Class entered into a contract with Apple for an iCloud+ subscription. Apple's representations concerning what iCloud+ included, including Private Relay and the protection Apple described it as providing, formed part of that agreement.

123. Plaintiff and the members of the Class performed their obligations by paying the subscription price.

124. Apple breached the agreement by failing to provide Private Relay conforming to the description under which it was sold.

125. Every contract governed by California law contains an implied covenant of good faith and fair dealing. Apple breached that covenant by charging for a privacy feature while withholding from subscribers that its own browser engine defeated the feature, thereby depriving subscribers of the benefit of their bargain.

126. Plaintiff and the members of the Class were damaged in the amount of the subscription fees paid for the protection they did not receive.

COUNT VII
UNJUST ENRICHMENT
(On Behalf of the Nationwide Class)

127. Plaintiff incorporates the allegations in paragraphs 1 through 79 by reference as if fully set forth herein.

128. This count is pleaded in the alternative to Count VI under Federal Rule of Civil Procedure 8(d).

130. Apple was aware of and accepted that benefit. Apple obtained those payments through representations concerning Private Relay that were false, and through the omission of material facts within Apple's exclusive knowledge.

131. It would be inequitable for Apple to retain the portion of those payments attributable to a privacy feature that did not deliver the represented protection.

8 132. Plaintiff seeks restitution and disgorgement of the amounts Apple unjustly retained.

3 133. Plaintiff incorporates the allegations in paragraphs 1 through 79 by reference as if
4 fully set forth herein.

134. The Florida Deceptive and Unfair Trade Practices Act (“FDUTPA”), Fla. Stat. §§ 501.201, et seq., prohibits unfair or deceptive acts or practices in the conduct of any trade or commerce. Fla. Stat. § 501.204.

135. Apple engaged in trade or commerce within the meaning of FDUTPA by advertising, marketing, offering, and selling iCloud+ subscriptions, including the Private Relay feature, to Plaintiff and members of the Florida Subclass.

136. Apple engaged in deceptive acts and practices by representing that Private Relay protects subscribers by routing their browsing requests through separate internet relays so that no single party, including the websites a subscriber visits, can see both who the subscriber is and what sites the subscriber visits.

137. Those representations were false or misleading because, as alleged herein, features of WebKit could bypass the Private Relay proxy path and transmit subscribers' real IP addresses or DNS queries outside Private Relay while the feature was enabled.

138. Apple further engaged in deceptive acts and practices by failing to disclose that its own browser engine contained pathways that bypassed Private Relay and thereby defeated the represented protection for those categories of network traffic. Apple possessed information concerning the operation of WebKit and Private Relay that was not reasonably available to consumers, while continuing to describe Private Relay in a manner that failed to disclose those limitations.

139. Apple's representations and omissions were likely to mislead consumers acting reasonably under the circumstances. A reasonable consumer purchasing a paid privacy feature represented to prevent websites from linking the consumer's identity to the websites the consumer visits would consider it material that features of Apple's own browser engine could transmit the consumer's real IP address or DNS queries outside the Private Relay architecture.

140. Apple's deceptive acts and practices caused Plaintiff and members of the Florida Subclass to suffer actual damages. Plaintiff and members of the Florida Subclass paid for iCloud+ subscriptions that included Private Relay as an advertised feature. Had iCloud+ and Private Relay possessed the characteristics and protections Apple represented, the subscriptions would have been worth more than the subscriptions Apple actually provided.

141. Plaintiff and members of the Florida Subclass therefore suffered actual damages measured by the difference between the market value of the iCloud+ subscription as represented and the market value of the subscription as actually provided, including the diminished value attributable to Private Relay's undisclosed bypass pathways.

142. Apple's deceptive acts and practices were a direct and proximate cause of these damages. Plaintiff and members of the Florida Subclass paid a price that reflected the represented

1 privacy protection, but received a service worth less because that protection did not function as
2 represented for the network traffic alleged herein.

3 143. Plaintiff, individually and on behalf of the Florida Subclass, seeks actual damages
4 pursuant to Fla. Stat. § 501.211(2), declaratory and injunctive relief pursuant to Fla. Stat. §
5 501.211(1), reasonable attorneys' fees and costs as provided by Fla. Stat. §§ 501.2105 and 501.211,
6 and all other relief available under FDUTPA.

7 8 **PRAYER FOR RELIEF**

9 **WHEREFORE**, Plaintiff, on behalf of Plaintiff and all others similarly situated, seeks
10 judgment against Apple as follows:

- 11 a) For an order determining that this action is properly brought as a class action, certifying
12 the Nationwide Class and Florida Subclass, appointing Plaintiff as class representative,
13 and appointing undersigned counsel as Class Counsel;
- 14 b) For an order declaring that Apple's conduct violated the statutes referenced herein;
- 15 c) For an order enjoining Apple from continuing the conduct alleged herein and requiring
16 Apple to correct its representations concerning iCloud Private Relay;
- 17 d) For compensatory damages in an amount to be determined at trial;
- 18 e) For restitution and disgorgement of all amounts Apple unjustly retained;
- 19 f) For punitive damages to the extent permitted by law;
- 20 g) For statutory damages and penalties to the extent available;
- 21 h) For pre-judgment and post-judgment interest on all amounts awarded;
- 22 i) For reasonable attorneys' fees and costs, including under Cal. Code Civ. Proc. section
23 1021.5; and

24 For such other and further relief as the Court deems just and proper.

DEMAND FOR TRIAL BY JURY

Plaintiff demands a trial by jury of all issues so triable.

Dated: August 14, 2026

Respectfully submitted,

/s/Jason M. Ingber

Jason M. Ingber (SBN 318323)

LEVI & KORSINSKY, LLP

3580 Wilshire Boulevard, Suite 1260

Los Angeles, California 90010-2513

Telephone: (213) 805-8373

Email: jingber@zlk.com

Mark Reich

Michael N. Pollack

LEVI & KORSINSKY, LLP

33 Whitehall Street, 27th Floor

New York, NY 10004

Telephone: (212) 363-7500

Facsimile: (212) 363-7171

Email: mreich@zlk.com

Email: mpollack@zlk.com

**pro hac vice forthcoming*

Counsel for Plaintiff