J. Aaron Lawson (SBN 319306)
alawson@edelson.com
Mickey Terlep (SBN 367340)
mterlep@edelson.com
EDELSON PC
150 California St., 18th Floor
San Francisco, California 94111
Tel: (415) 212-9300

Attorneys for Plaintiffs

Per local Rule, This case is assigned to Judge Reyes, Benjamin T, II, for all purposes.

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF CONTRA COSTA

DORIAN ELDRIDGE and SILAS PEREZ, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

FLOCK GROUP INC.,

Defendant.

Case No.: C26-00576

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

SUMMONS ISSUED

Plaintiffs Dorian Eldridge and Silas Perez bring this Class Action Complaint and Demand for Jury Trial against Defendant Flock Group Inc., and allege as follows upon personal knowledge as to themselves and their own acts and experiences, and upon information and belief as to all other matters:

NATURE OF THE ACTION

1. Flock operates one of the largest automated license plate recognition ("ALPR") networks in the country. Its cameras, which are mounted on unmarked poles along public roads throughout California, photograph nearly every passing vehicle and capture license plate numbers, vehicle images, and the precise location, date, and time of each sighting. That data is uploaded to Flock's centralized databases, where it can be searched, aggregated, and shared across Flock's network of more than 4,800 law enforcement agency clients. The result is a surveillance system that tracks the movements of millions of Californians—including data showing where they live,

work, worship, seek medical care, protest, and associate—without their knowledge or even a warrant.

2. California law does not prohibit ALPR surveillance. But the Legislature recognized that unchecked ALPR use capturing the movements of millions of drivers, continuously and without notice, demands meaningful regulation. In 2015, the Legislature enacted Senate Bill No. 34 (2015-2016 Reg. Sess.) (hereafter "SB 34" or the "ALPR Law") to regulate how ALPR data is collected, secured, and shared with third parties. (Civ. Code, § 1798.90.5 et seq.) SB 34 requires ALPR operators like Flock to maintain reasonable security procedures, implement and post a "usage and privacy policy," and ensure that ALPR data is used only for "authorized purposes." SB 34 also prohibits California public agencies from sharing ALPR data with federal agencies and out-of-state law enforcement. (See Civ. Code, § 1798.90.5, subd. (f); § 1798.90.55, subd. (b).)

3. The First Appellate District recently confirmed that these obligations are mandatory. In *Bartholomew v. Parking Concepts, Inc.*, the court recognized that the public-facing disclosure is a "primary focus of the ALPR Law" because the statute "grants individuals the right to know which entities are collecting their ALPR data and how it is being used and maintained." The court held that collecting ALPR data without a compliant policy is itself a cognizable harm under the statute—meaning that Flock is systematically violating the privacy and civil liberties of millions of California residents on thousands of roads across the state, every single day. (See *Bartholomew*, (Ct.App. Feb. 5, 2026, No. A171546) 2026 WL 308163, at *6 ("Collecting and maintaining individuals' ALPR information without implementing and making public the statutorily required policy harms these individuals by violating this right to know.").)

4. Flock has systematically violated these statutory obligations, and its conduct has far-reaching consequences. The ALPR information Flock collected on California drivers—and then made available to unauthorized agencies nationwide—has been exploited for exactly the purposes the Legislature sought to prevent. Flock's ALPR information has been used for a number of unlawful purposes, including federal immigration enforcement, cross-border investigations targeting women who obtained abortions, and dragnet surveillance untethered from any criminal predicate.

5. Flock designed its system—including the cross-jurisdictional sharing features like "National Lookup"—to facilitate exactly the kind of sharing SB 34 prohibits. A single lookup on Flock's platform can sweep across its entire nationwide database, giving federal and out-of-state agencies, including Immigration and Customs Enforcement ("ICE") broad access to California ALPR information. The scope of this unlawful sharing only came to light through investigative reporting and public records requests, which revealed systematic violations across California. More than 1.6 million searches were conducted by 5,757 outside agencies—including at least 19 searches marked as related to ICE operations—on ALPR information collected by the San Francisco Police Department, which was just one of more than 200 California agencies on Flock's platform. Texas law enforcement used Flock's network to conduct a nationwide search, including specifically in California, for a woman they claimed had obtained an abortion. Audit logs reflect discriminatory search terms and cross-border investigations related to abortion and other sensitive medical care.

6. In February 2025, Flock acknowledged that out-of-state agencies had access to conduct broad searches of California ALPR data. But it was only after sustained public scrutiny that Flock finally removed California from its "National Lookup" system. Even then, numerous law enforcement agencies in California continued to use Flock's system to share California ALPR data with federal and other out-of-state agencies.

7. As discussed more fully below, Flock violated SB 34 in two distinct ways.

8. First, it failed to post the required "usage and privacy policy" before collecting ALPR information from California drivers. SB 34 requires that ALPR operators identify the "authorized purposes" for collecting and using ALPR information. "The authorized uses delineated in the policy apply not only to the ALPR operator, but to anyone who receives ALPR information from that operator." (*Bartholomew, supra*, 2026 WL 308163, at *6.) SB 34 also requires that the policy include a description of how the ALPR system is monitored for compliance with privacy laws, who is authorized to access the system, what training they receive, and the "purposes of, process for, and restrictions on" the sale or sharing of ALPR information to third parties. (See Civ. Code, § 1798.90.51, subd. (b)(2)(D).) Flock's publicly posted policy fails

on every count.

9. Second, Flock designed its system to make California ALPR information available to federal agencies and out-of-state law enforcement. Flock's "National Lookup" and cross-jurisdictional sharing features allowed any agency on its platform to search California ALPR databases without restriction. Flock implemented no technical safeguards to limit access to California public agencies as the statute requires, did not require multifactor authentication, and did not provide California agencies with the ability to block unauthorized access to their data.

10. Plaintiffs are California residents whose vehicles were photographed by Flock ALPR cameras and whose ALPR information was captured and stored on Flock's system. Their data was accessible to federal agencies, out-of-state law enforcement, and the public at large in violation of SB 34. They bring this action on behalf of themselves and a class of similarly situated California residents to hold Flock accountable for its knowing violations of Civil Code sections 1798.90.5 et seq.

PARTIES

11. Plaintiff Dorian Eldridge is a natural person and citizen of the State of California. Plaintiff Eldridge resides in the City of San Ramon.

12. Plaintiff Silas Perez is a natural person and citizen of the State of California. Plaintiff Perez resides in the City of Monrovia.

13. Defendant Flock Group Inc. is a corporation formed under the laws of Delaware, with its principal place of business in Georgia.

JURISDICTION AND VENUE

14. This Court has subject matter jurisdiction over this matter pursuant to Article VI, section 10 of the California Constitution.

15. This Court has general personal jurisdiction over Flock because Flock conducts substantial, continuous, and systematic business in California. Flock has active contracts with more than 200 California law enforcement agencies, including the San Ramon Police Department and Contra Costa Sheriff's Office, operates thousands of ALPR cameras within the state, and collects and stores data on millions of California drivers. Plaintiffs' claims arise out of and relate

to Flock's California contacts.

16. Venue is proper in Contra Costa County under Code of Civil Procedure section 395, subdivision (a) because Plaintiff Eldridge resides in Contra Costa County, Flock operates ALPR cameras in Contra Costa County, and a substantial part of the events giving rise to Plaintiff Eldridge's claims occurred in this County.

FACTUAL BACKGROUND

I. The California ALPR Law.

17. In 2015, the California Legislature recognized the numerous privacy concerns implicated by the use of ALPR technology:

> The collection of a license plate number, location, and time stamp over multiple time points can identify not only a person's exact whereabouts but also their pattern of movement. Unlike other types of personal information that are covered by existing law, civilians are not always aware when their ALPR data is being collected. One does not even need to be driving to be subject to ALPR technology: A car parked on the side of the road can be scanned by an ALPR system. This bill will put in place minimal privacy protections by requiring the establishment of privacy and usage protection policies for ALPR operators and end users.

18. To address these concerns the ALPR law requires ALPR operators (such as Flock), and end users (such as law enforcement agencies), to comply with three basic requirements:

i. *The Security Requirement*: ALPR operators and end users must "[m]aintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure." (Civ. Code, § 1798.90.51, subd. (a); § 1798.90.53, subd. (a).)

ii. *The Privacy Requirement*: ALPR operators and end users must implement a usage and privacy policy in order to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties. (Civ. Code, § 1798.90.51, subd. (b)(1); § 1798.90.53, subd. (b)(1).)

iii. *The Notice Requirement*: ALPR operators and end users must post a usage and privacy policy "conspicuously" on their website and include the following information

pursuant to Civil Code sections 1798.90.51, subdivision (b) and 1798.90.53, subdivision (b):

(a) The authorized purposes for using the ALPR system and collecting ALPR information;

(b) A description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR system, or to collect ALPR information. The policy shall identify the training requirements necessary for those authorized employees and independent contractors;

(c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws;

(d) The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons;

(e) The title of the official custodian, or owner, of the ALPR system responsible for implementing this section;

(f) A description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors; and

(g) The length of time ALPR information will be retained, and the process the ALPR operator will utilize to determine if and when to destroy retained ALPR information.

19. ALPR operators must also comply with two additional requirements to ensure consumer privacy and protect against unauthorized access:

i. *The Audit Requirement*. ALPR operators must maintain a record of the times their ALPR system is accessed, whether by operators, employees, or end users. (Civ. Code, § 1798.90.52, subd. (a).) The audit trail must note the date and time of the query, the data that was queried, who queried it, and the purpose of the query. (*Ibid*.) A record that omits required fields or uses non-descriptive placeholders for "purpose"—for example, a blank entry or a generic label such as "investigation"—defeats the auditability SB 34

mandates and undermines the Legislature's intent that ALPR access be meaningfully reviewable and accountable.

ii. *The Proper Use Requirement*. ALPR operators must also "[r]equire that ALPR information only be used for the authorized purposes described in the usage and privacy policy." (Civ Code., §1798.90.52, subd. (b).)

20. California public agencies collecting ALPR data may not share ALPR data with federal agencies or out-of-state law enforcement agencies. "A public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law." (Civ. Code., § 1798.90.55, subd. (b).) "Public agency" means "the state, any city, county, or city and county, or any agency or political subdivision of the state or a city, county, or city and county, including, but not limited to, a law enforcement agency." (Civ. Code., § 1798.90.5, subd. (f).)

21. The California Attorney General issued written guidance in October 2023 explaining that the plain text of the ALPR Law permits the sharing of ALPR data *only* with other California state and local agencies:

> [T]he definition of "public agency" is limited to state or local agencies, including law enforcement agencies, and does not include out-of-state or federal law enforcement agencies. (See Civ. Code, § 1798.90.5, subd. (f).) Accordingly, SB 34 does not permit California LEAs [Law Enforcement Agencies] to share ALPR information with private entities or out-of-state or federal agencies, including out-of-state and federal law enforcement agencies. This prohibition applies to ALPR database(s) that LEAs access through private or public vendors who maintain ALPR information collected from multiple databases and/or public agencies.

22. Likewise, the California AG has clarified that, under SB 34, "ALPR operators [like Flock] . . . must develop a usage and privacy policy, which must be conspicuously posted on their website, and must contain provisions designed to 'protect ALPR information from unauthorized access, destruction, use, modification, or disclosure.'"

23. An individual harmed by this statute may bring a civil suit "against a person who knowingly caused the harm" and recover (1) actual damages, but not less than liquidated damages in the amount of $2,500, (2) punitive damages upon proof of willful or reckless disregard of the law, (3) reasonable attorney's fees and other litigation costs reasonably incurred, and (4) other

preliminary and equitable relief as the court determines to be appropriate. (Civ. Code, § 1798.90.54, subd. (b).)

II. Flock's ALPR System and Unlawful Practices.

24. Flock operates one of the largest ALPR systems in the United States. Flock's system includes thousands of cameras deployed throughout California, a centralized database containing billions of license plate scans, and an AI-powered software platform that enables real-time searching, analysis, and cross-jurisdictional data sharing.

25. Flock's most popular products, the "Falcon" and the "Sparrow," are ALPR cameras that photograph all passing vehicles. The cameras are typically mounted on existing traffic poles or on freestanding unmarked poles with solar power sources.

26. Flock ALPR cameras collect the following information: (a) license plate image; (b) vehicle image; (c) vehicle characteristics (including color, make, body type, and other visual details such as bumper damage, roof racks, and stickers); (d) license plate number; (e) license plate state; (f) date; (g) time; and (h) camera location.

27. Flock uses machine learning to identify and analyze vehicles beyond basic license plate recognition. Flock refers to this composite identifying information as a "Vehicle Fingerprint." Flock has stated in its own marketing materials that its system "delivers more than just license plate information" and that it has "taken license plate reading to the next level by including details on the entire vehicle," including the ability to "identify a temporary paper plate and even a vehicle where there is no plate present."

28. Flock holds a United States patent (U.S. Patent No. 11,416,545 B1) for a dynamic surveillance system that can be configured to identify "classes of people (male, female, race, etc.)." While Flock claims in advertising materials that it does not use facial recognition, recent reporting indicates that Flock's ALPR readers in at least some instances capture images of people's faces, saving them to a folder separate from the ALPR data.

29. More than 200 California law enforcement agencies collect and use images captured by Flock ALPR cameras. The Los Angeles County Sheriff's Department alone operates 476 Flock cameras.

30. Flock boasts that its cameras are used by more than 4,800 law enforcement agencies nationwide and claims to operate the nation's largest fixed ALPR network: "With billions of monthly plate reads, Flock connects communities, businesses and law enforcement in a shared network."

31. Flock does not merely collect data passively. Its AI-powered system analyzes movement patterns, identifies how often a vehicle visits a given location, and can predict future activity based on historical data. In 2025, Flock announced new capabilities through its "Investigations Manager" product, designed to proactively flag vehicles as suspicious. These features include a "Multi-State Insights" feature that alerts law enforcement when vehicles are detected in multiple states; a "Linked Vehicles" or "Convoy Search" that allows police to uncover vehicles frequently seen together; and a "Multiple locations search" that identifies vehicles seen at multiple locations.

A. Flock Disclosed California ALPR Data to Federal and Out-of-State Agencies.

32. Despite the ALPR Law's clear prohibition on sharing California ALPR data with non-California entities, Flock allows federal agencies—including ICE—and numerous out-of-state law enforcement agencies, to access its California ALPR databases.

33. Flock's system includes a "National Lookup" feature that permits law enforcement agencies outside of California to search a given California agency's ALPR data.

34. Only after extensive negative media coverage in mid-2025 did Flock remove California ALPR information from its national lookup system. The timing of this change amounts to a tacit admission that Flock's configuration violated California law.

35. Before and even after this change, California law enforcement agencies used Flock's platform to search ALPR data on behalf of federal agencies in direct violation of the ALPR Law.

36. In February 2025, Flock acknowledged to California agencies that its system architecture permitted out-of-state law enforcement agencies to conduct broad searches of California ALPR data.

37. Even after Flock's mid-2025 system changes, violations continued. Officers from the San Francisco and Oakland Police Departments continued sharing California Flock ALPR data with at least seven federal agencies. Many California agencies that had previously run illegal immigration-related searches subsequently ran hundreds of searches with no case number and no stated reason beyond "investigation," raising concerns that unlawful sharing persists.

38. The Riverside County Sheriff's Department continued to perform ALPR searches on behalf of federal agencies even after being informed that its practice of sharing ALPR data with federal agencies violated state law.

39. A 2023 analysis by the Electronic Frontier Foundation found that at least 71 California law enforcement agencies had violated the ALPR Law that year.

40. The California Attorney General has initiated enforcement actions against at least 20 California law enforcement agencies, and in October 2025 filed suit against the City of El Cajon for illegally sharing license plate data with out-of-state law enforcement.

41. Flock's system architecture made these violations foreseeable and preventable. As Flock itself has acknowledged, once a department allows another agency to access its system, the outside agency can search the data without needing approval each time. Users can query multiple networks simultaneously: searches of Oakland's ALPR data were found to reach hundreds of other networks at once.

B. Flock Failed to Implement an Adequate Privacy and Usage Policy.

42. The ALPR Law requires ALPR operators to implement a usage and privacy policy designed to ensure that ALPR data collection, use, and sharing is "consistent with respect for individuals' privacy and civil liberties" and to monitor the system to ensure "compliance with applicable privacy laws." (Civ. Code, §§ 1798.90.51, subds. (b)(1), (b)(2)(C).)

43. As the *Bartholomew* court held, this policy requirement is "critical in holding ALPR operators accountable[.]" (*Bartholomew*, *supra,* 2026 WL 308163, at *6.) Without a compliant policy establishing authorized uses, "it is much more difficult to hold them accountable for *unauthorized* uses, even though this is an example of a harm-causing violation expressly stated in the ALPR Law." (*Ibid.* (emphasis in original).)

44. Flock's policy, as it existed for the majority of the class period, did not include adequate provisions to prevent unauthorized sharing of California ALPR data with federal or out-of-state agencies. Until at least June 2025, Flock's system permitted national lookups that exposed California data to non-California agencies without any safeguard or warning.

45. Flock has publicly disclaimed responsibility for compliance with the ALPR Law, maintaining that its "customers choose whether to share LPR data with other customers in accordance with their laws and policies." This position is contrary to the ALPR Law, which imposes independent obligations on ALPR operators—not just end users—to ensure compliance with applicable privacy laws. (See Civ. Code, § 1798.90.51, subd. (b)(2)(C) [policy must describe "how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws"]; see also Civ. Code, § 1798.90.52, subd. (b) [operator must "require that ALPR information only be used for the authorized purposes"].)

46. Flock's CEO Garrett Langley, in a June 2025 blog post announcing the removal of California from national lookup, characterized the change as intended "to make compliance easier"—language that falls well short of the ALPR Law's mandate that operators ensure compliance.

47. In an August 2025 blog post, Langley wrote that Flock's new Chief Legal Officer would lead efforts "to ensure users are able to determine, in compliance with local laws, regulations, and community norms, whether and when to share their data." This statement is an implicit admission that, prior to that date, Flock's system did not enable users to comply with California law, and that Flock was not in compliance with the ALPR Law. It also confirms that it was always feasible for Flock to place reasonable limitations on use of its database in order to comply with California law.

C. Flock Failed to Maintain Reasonable Security Procedures.

48. The ALPR Law requires ALPR operators to "[m]aintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure." (Civ. Code, § 1798.90.51, subd. (a).)

49. Flock's security practices fall far below any reasonable standard.

50. Failure to Require Multifactor Authentication. Flock did not require multifactor authentication ("MFA") for law enforcement end users accessing its ALPR database. MFA is a basic, widely adopted security measure used to protect access to sensitive systems, including the federal courts' PACER filing system. Flock's failure to mandate MFA facilitated unauthorized credential sharing with federal and out-of-state agencies. Only after negative press coverage did Flock make MFA a default setting—but even then, Flock still did not require it. Predictably, Flock police login credentials have been found for sale by Russian hackers on dark web forums.

51. Fifty-One Identified Vulnerabilities. A security researcher known as Jon "GainSec" Gaines published a formal white paper identifying fifty-one vulnerabilities in Flock's hardware and software, many classified as critical. These include:

(a) *Physical vulnerabilities*: Pressing an easily accessible button on the back of publicly mounted Flock cameras in a simple sequence opens a wireless access point that can be hijacked to grant root access to the camera's systems, enabling an attacker to access video data, scrape data, insert fake camera feeds, obtain police information, and install software. Exposed USB ports provide yet another avenue for unauthorized access.

(b) *Unsupported operating system*: Flock cameras continue to run on Android Things 8.1, a mobile operating system that has been discontinued by Google and is no longer supported with security patches.

(c) *Unprotected testing data*: Flock left its internal testing data accessible online, including police names, phone numbers, patrol areas, suspect hotlists, full license plates, and geographic information systems data showing the live locations of patrol cars.

(d) *Exposed Video Feeds*. Reporting revealed that video feeds from Flock's "Condor" cameras—designed to track people and operating in conjunction with Flock's ALPR cameras—were configured in a way that made at least dozens of live feeds accessible on the internet without any password or login information.

Several of these unsecured feeds were from cameras located in California. Journalists were able to watch in real time as Flock's devices surveilled drivers and pedestrians.

(e) *Leaked Audit Reports*. Flock's monthly audit reports, which are subject to public records requests, have revealed hundreds of thousands of unredacted license plate numbers, alongside the sensitive reasons law enforcement agencies searched for them. Rather than implementing proper redaction procedures, Flock removed wholesale the ability to view officer names and license plate numbers from audit reports—rendering the reports insufficient under Civil Code section 1798.90.52, subdivision (a), while failing to address the underlying security deficiency.

52. Flock's response to the GainSec white paper was misleading. Flock claimed that exploitation of the identified vulnerabilities would "require physical access to a device" and "intimate knowledge of internal device hardware." But Flock's cameras are mounted in public areas, making physical access easy, and the white paper itself noted that the vulnerabilities could be exploitable by less experienced hackers.

D. Flock's Audit and Transparency Failures Enabled Unauthorized Use and Disclosure.

53. SB 34's audit requirement exists to ensure ALPR operators maintain an auditable record of access and use—including "[t]he purpose for accessing the information"—so that unauthorized or unlawful searches can be detected, investigated, and deterred. (See Civ. Code, § 1798.90.52, subd. (a).) The audit requirement is a critical accountability mechanism: it enables oversight by regulators and the public, and it deters misuse by ensuring that those who access ALPR information know their searches will be recorded and reviewable. By failing to maintain adequate audit records, an ALPR operator deprives individuals of the statutory protection designed to ensure that access to their ALPR information is transparent and accountable.

54. Flock's platform generates and provides monthly audit reports to end-user agencies. Those audit reports have been routinely subject to public records requests. Reporting has

revealed that audit-report disclosures exposed large quantities of unredacted license plate numbers alongside the sensitive reasons officers searched for them. This information can be used to infer where individuals live, work, worship, associate, and seek medical care.

55. These disclosures were foreseeable. SB 34 requires maintenance of audit records, and California public-records laws make it predictable that agencies will receive—and respond to—requests for audit materials. Reasonable ALPR security and privacy practices therefore require robust operational and technical controls to ensure audit materials can be produced in compliance with public-records obligations without disclosing ALPR information to the public at large.

56. Instead of implementing reasonable and privacy-protective redaction and access controls, Flock's response has been to remove (or materially degrade) core audit fields—including officer names and license plate numbers—in a manner that renders audit reports insufficient for SB 34 oversight while leaving unchanged the system's underlying susceptibility to unauthorized access, misuse, and disclosure.

57. The audit materials and public reporting also reflect widespread access that Flock failed to prevent. Even after public scrutiny of unlawful federal and out-of-state access, many agencies ran searches with no case number and no reason beyond "investigation," which shows that prohibited sharing and unauthorized use continues to persist.

58. Public reporting of Flock audit logs have also documented uses that heighten the intrusion and offensiveness of this surveillance, including discriminatory search terms and cross-border investigations related to abortion and other sensitive medical care. These examples underscore why SB 34 requires ALPR operators not only to keep meaningful audit records, but also to require that ALPR information be used only for authorized purposes and to prevent unauthorized access and disclosure.

III. Plaintiff Eldridge.

59. Plaintiff Eldridge drives a vehicle registered in California and regularly drives on public roads in San Ramon and Contra Costa County.

60. Flock operates ALPR cameras in areas where Plaintiff regularly drives, including within San Ramon, Contra Costa County, and surrounding areas.

61. On information and belief, Flock ALPR cameras have captured images of Plaintiff's vehicle since at least 2023, including his license plate number, vehicle image, vehicle characteristics, and the location, date, and time of each capture.

62. On information and belief, Plaintiff's ALPR data was stored in Flock's database during a period when that database was accessible to federal agencies and out-of-state law enforcement agencies.

63. In 2024, Plaintiff Eldridge was driving his vehicle in California when a law enforcement officer initiated a traffic stop. The officer told Plaintiff Eldridge that the stop was initiated because his license plate was flagged by Flock as a stolen vehicle. The officer later determined that Flock flagged Plaintiff Eldridge's license plate in error.

64. Plaintiff had no knowledge that Flock's system permitted the unauthorized sharing of his ALPR data until recently, when public reporting revealed the scope of Flock's violations.

65. Plaintiff's ALPR data was captured covertly by cameras mounted on public infrastructure as he drove on public roads. Plaintiff could not have avoided Flock's collection of his ALPR data other than by refraining from driving entirely.

66. Plaintiff has been harmed by Flock's conduct. This harm includes, but is not limited to: (a) the unauthorized access to his ALPR information by federal and out-of-state agencies; (b) the collection and use of his ALPR information without Flock having implemented an adequate, publicly available usage and privacy policy; (c) the violation of his right to know which entities are collecting his ALPR data and how it is being used and maintained; and (d) the ongoing risk that his ALPR data will continue to be accessed, used, or shared by unauthorized parties.

IV. Plaintiff Perez.

67. Plaintiff Perez drives a vehicle registered in California and regularly drives on public roads in Monrovia and Los Angeles County.

68. Flock operates ALPR cameras in areas where Plaintiff Perez regularly drives, including within Monrovia, Los Angeles County, and surrounding areas.

69. On information and belief, Flock ALPR cameras have captured images of Plaintiff's vehicle since at least 2023, including his license plate number, vehicle image, vehicle characteristics, and the location, date, and time of each capture.

70. On information and belief, Plaintiff's ALPR data was stored in Flock's database during a period when that database was accessible to federal agencies and out-of-state law enforcement agencies.

71. At no point did Plaintiff authorize Flock or any law enforcement agency to share his ALPR data with federal agencies or out-of-state law enforcement agencies.

72. Plaintiff had no knowledge that Flock's system permitted the unauthorized sharing of his ALPR data until recently, when public reporting revealed the scope of Flock's violations.

73. Plaintiff's ALPR data was captured covertly by cameras mounted on public infrastructure as he drove on public roads. Plaintiff could not have avoided Flock's collection of his ALPR data other than by refraining from driving entirely.

74. Plaintiff has been harmed by Flock's conduct. This harm includes, but is not limited to: (a) the unauthorized access to his ALPR information by federal and out-of-state agencies; (b) the collection and use of his ALPR information without Flock having implemented an adequate, publicly available usage and privacy policy; (c) the violation of his right to know which entities are collecting his ALPR data and how it is being used and maintained; and (d) the ongoing risk that his ALPR data will continue to be accessed, used, or shared by unauthorized parties.

CLASS ALLEGATIONS

75. **Class Definition**. Pursuant to Code of Civil Procedure section 382, Plaintiff brings this action on behalf of himself and a class of similarly situated individuals (the "Class"), defined

as:

> All California residents whose license plate data was collected by Flock in the State of California using an automated license plate recognition system operated by Flock.

Excluded from the Class are: (1) any judicial officer presiding over this matter, members of their immediate families, and judicial staff; (2) Defendants, their affiliates, parents, subsidiaries, employees, officers, and directors; (3) any governmental entity; and (4) persons who properly execute and file a timely request for exclusion from the Class. Plaintiff reserves the right to modify or expand the Class definition as warranted by facts learned through investigation and discovery.

76. **Numerosity**. Members of the Class are so numerous that their individual joinder is impracticable. On information and belief, Flock has photographed the license plates and location data of tens of millions of California drivers. More than 200 California law enforcement agencies use Flock's ALPR cameras, and the Los Angeles County Sheriff's Department alone operates 476 Flock cameras. The Class is estimated to include millions of individuals. Class Members may be notified of the pendency of this action by mail, email, and/or publication.

77. **Commonality and Predominance**. There are many questions of law and fact common to the claims of Plaintiffs and the putative Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include, but are not necessarily limited to the following:

(a) Whether Flock is an "ALPR operator" and/or "ALPR end-user" under SB 34;

(b) Whether Flock implemented and conspicuously posted a usage and privacy policy that satisfies Civil Code section 1798.90.51, subdivision (b);

(c) Whether Flock required that ALPR information be used only for authorized purposes as required by Civil Code section 1798.90.52, subdivision (b);

(d) Whether Flock designed or configured its system in a manner that made California ALPR information accessible to federal agencies and out-of-state law enforcement agencies;

(e) Whether Plaintiffs and Class Members were harmed by Flock's conduct; and

(f) Whether punitive damages are warranted.

78. **Adequate Representation**. Plaintiffs will fairly and adequately represent and protect the interests of the Class and have retained counsel competent and experienced in complex litigation and class actions. Plaintiffs' claims are representative of the claims of the other members of the Class. That is, Plaintiffs and the Class members sustained damages as a result of Defendant's conduct. Plaintiffs also have no interests antagonistic to those of the Class, and Defendant has no defenses unique to Plaintiffs. Plaintiffs and their counsel are committed to vigorously prosecuting this action on behalf of the members of the Class and have the financial resources to do so. Neither Plaintiffs nor their counsel have any interest adverse to the Class.

79. **Predominance and Superiority**. Class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, as joinder of all members of the Class is impracticable. Individual litigation would not be preferable to a class action because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. Economies of time, effort, and expense will be fostered and uniformity of decisions will be ensured.

80. Plaintiff reserves the right to revise the foregoing "Class Allegations" and "Class Definition" based on facts learned through additional investigation and in discovery.

FIRST CAUSE OF ACTION
Violation of Civ. Code, § 1798.90.51, subd. (b)
(Failure to Implement and Conspicuously Post a Compliant Usage and Privacy Policy)
(By All Plaintiffs Against Defendant)

81. Plaintiffs incorporate the foregoing allegations as though fully set forth herein.

82. Flock is an "ALPR operator" under Civil Code section 1798.90.5, subdivision (c) because it operates an ALPR system consisting of a searchable computerized database resulting from the operation of thousands of fixed cameras combined with computer algorithms to read and convert images of license plates and the characters they contain into computer-readable data. Flock is also an "ALPR end-user" under Civil Code section 1798.90.5, subdivision (a) because it accesses and uses ALPR data, including for training its artificial intelligence algorithms.

83. Civil Code section 1798.90.51, subdivision (b)(1) requires ALPR operators to implement "a usage and privacy policy in order to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties," and provides that "[t]he policy shall be available to the public in writing, and, if the ALPR operator has an Internet Web site, the usage and privacy policy shall be posted conspicuously on that Internet Web site."

84. Civil Code section 1798.90.51, subdivision (b)(2) requires that the policy address, at minimum: (A) "The authorized purposes for using the ALPR system and collecting ALPR information"; (B) the job title/designation of authorized employees/contractors and the training requirements necessary for those authorized employees/contractors; (C) monitoring to ensure security and "compliance with applicable privacy laws"; (D) "The purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons"; (E) the title of the official custodian/owner responsible for implementing the section; (F) accuracy and correction of data errors; and (G) retention length and the process for determining if and when to destroy retained ALPR information.

85. The Court of Appeal has held that the ALPR Law "grants individuals *the right to know* which entities are collecting their ALPR data and how it is being used and maintained." (*Bartholomew, supra*, 2026 WL 308163, at *6.)

86. Flock collects, uses, maintains, shares, and disseminates ALPR information while posting on its website a document titled "License Plate Reader Policy" that purports to be its "Flock Safety License Plate Reader Usage and Privacy Policy," which is "Last Updated: November 13, 2025." (Flock Safety, *License Plate Reader Policy* (last updated Nov. 13, 2025).)

87. Flock's posted License Plate Reader Policy ("LPR Policy") is not compliant with Civil Code section 1798.90.51, subdivision (b) because it does not provide the public the statutorily required disclosures that give effect to the right to know "which entities are collecting their ALPR data and how it is being used and maintained." (*Bartholomew, supra*, 2026 WL 308163, at *6.)

I. Failure to Disclose "Authorized Purposes."

88. Section 1798.90.51, subdivision (b)(2)(A) requires the policy to state "[t]he authorized purposes for using the ALPR system and collecting ALPR information." Flock violates this requirement in three ways.

89. First, Flock's posted LPR Policy fails to identify any "authorized purposes" in the policy itself, and instead, points individuals to a separate document for the statutorily-required information:

> **Authorized Purposes:** The purpose of Flock Safety's LPR system is defined under "Permitted Purpose" in Flock Safety's Terms and Conditions.

90. Second, even if the ALPR Law permitted operators to direct individuals to a separate document for "authorized purposes" disclosures—which it does not—Flock's Terms and Conditions are a private agreement between Flock and its law enforcement customers, not a public-facing disclosure to the individuals whose data is being collected. California drivers are not required to parse through the terms of a third-party business contract to ascertain critical information that Flock was required to disclose through the LPR Policy.

91. Third, the Terms and Conditions in the private agreement between Flock and its law enforcement customers define "Permitted Purpose" so broadly as to render the disclosure meaningless. "Permitted Purpose" is defined as any "legitimate public safety and/or business purpose, including the awareness, prevention, and prosecution of crime; investigations; and prevention of commercial harm, to the extent permitted by law."

92. This definition places no operative boundary on the use of ALPR information. As *Bartholomew* recognized, SB 34's transparency requirement exists to give individuals "*the right to know* which entities are collecting their ALPR data and how it is being used and maintained." (*Bartholomew, supra,* 2026 WL 308163, at *6.) That right is defeated when the stated "authorized purposes" amount to anything a law enforcement agency or private customer decides qualifies as a public safety or business purpose—limited only by the circular constraint that the use be "permitted by law."

93. And in any event, Flock continues to this day to allow federal and out-of-state agencies to access California ALPR information in clear violation of SB 34.

II. Failure to Identify Job Title and Training Requirements for Authorized Employees.

94. Section 1798.90.51, subdivision (b)(2)(B) requires the policy to include "[a] description of the job title or other designation of the employees and independent contractors who are authorized to use or access the ALPR system, or to collect ALPR information," and provides that, "[t]he policy shall identify the training requirements necessary for those authorized employees and independent contractors."

95. Flock's posted policy does not describe the job titles or designations of authorized employees or independent contractors. It states only: "Each Flock Safety customer designate one or more 'administrators' who are the custodians and head administrators of the LPR systems and its operation. Each customer's data is accessible to the administrator(s) and authorized end-users (together, 'users')."

96. The policy further states: "To provide customer support and address system issues, Flock Safety has designated CJIS-certified engineers who are able to access CJIS data and other designated individuals who are able to access other system data ('privileged administrators')."

97. These statements do not identify the required job titles or designations of the employees and independent contractors authorized to use or access the system or collect ALPR information. They also do not identify who, by title or designation, constitutes "authorized end-users," "designated individuals," or "privileged administrators."

98. The policy also fails to identify the training requirements necessary for authorized employees and independent contractors. It states only: "Training: Flock Safety provides training to LPR system users on the proper use of the system. Flock Safety encourages customers to implement additional training for its users. Flock Safety employees are required to complete regular cybersecurity trainings."

99. This generalized "provides training" and "encourages" language does not identify the training requirements necessary for authorized employees and independent contractors, as required by section 1798.90.51, subdivision (b)(2)(B), and does not provide the public with the

required disclosures about who is authorized and what training they must have before collecting, accessing, or using ALPR information.

III. Failure to Describe Monitoring to Ensure Compliance With Applicable Privacy Laws.

100. Section 1798.90.51, subdivision (b)(2)(C) requires "[a] description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws."

101. Flock's posted policy provides a generic list of security statements—such as, "Flock Safety's information security policy and safeguards align with the security requirements established by NIST Cybersecurity and CISA Secure By Design"—but fails to describe how the system will be monitored to ensure "compliance with applicable privacy laws," including SB 34's restrictions on sharing California ALPR information with non-California entities.

102. Instead, Flock shifts its statutory obligation to monitor compliance with privacy laws to its customers: "This data is stored in the Flock Safety system to facilitate audits conducted according to the policies of each Flock Safety customer, in order to ensure access was made by authorized persons for legitimate purposes and in compliance with law and policy. Flock Safety encourages customers to adopt a use policy and implement a regular auditing schedule."

103. This is not the monitoring-for-compliance disclosure SB 34 requires. It fails to explain how Flock monitors cross-jurisdictional access, sharing pathways, and other high-risk uses to ensure compliance with California privacy laws, and fails to provide the public with the required description of monitoring for legal compliance.

IV. Failure to Identify Purposes/Process/Restrictions on Sharing of ALPR Information.

104. Section 1798.90.51, subdivision (b)(2)(D) requires "[t]he purposes of, process for, and restrictions on, the sale, sharing, or transfer of ALPR information to other persons."

105. Flock's policy does not describe the required process or restrictions. It states: "**Restrictions on the Sale, Sharing, or Transfer of LPR Data:** LPR data gathered by the Flock Safety system on behalf of Flock Safety customers is owned by the customer. Customers choose

whether to share LPR data with other customers in accordance with their laws and policies."

106. This language does not describe the "process for" and "restrictions on" its customers' "sale, sharing, or transfer of ALPR information to other persons," as required by section 1798.90.51, subdivision (b)(2)(D).

107. Finally, the policy discloses a separate use of ALPR images for machine learning: "Additionally, Flock uses a fraction of LPR images (less than one percent), which are stripped of all metadata and identifying information, solely for the purpose of improving Flock Services through machine learning." Flock's Privacy Policy similarly defines "Training Data" as: "a small fraction (less than 1%) of images captured by the Flock Services, which are stripped of all metadata and identifying information, for the limited purpose of improving our products and services through machine learning."

108. This machine-learning use is a purpose for collecting and using ALPR information that must be transparently disclosed in a statutorily compliant usage and privacy policy. Flock's policy does not describe the process for selecting such images, the restrictions on this use, or how compliance with applicable privacy laws is ensured.

V. Failure to Describe Measures For Correcting Data Errors.

109. Section 1798.90.51, subdivision (b)(2)(F) requires "[a] description of the reasonable measures that will be used to ensure the accuracy of ALPR information and correct data errors."

110. Flock's policy altogether fails to describe reasonable measures that will be used to "correct data errors," including what happens to inaccurate reads, what mechanisms exist to identify, correct, annotate, or purge inaccurate information, or how affected individuals' data errors are corrected. Flock therefore fails to comply with section 1798.90.51, subdivision (b)(2)(F).

VI. Failure to Describe Retention/Destruction Process.

111. Section 1798.90.51, subdivision (b)(2)(G) requires "[t]he length of time ALPR information will be retained, and the process the ALPR operator will utilize to determine if and when to destroy retained ALPR information."

112. Flock's posted policy states: "LPR data is hard deleted on a rolling 30-day basis by default" but goes on to say that its retention of ALPR information "may be increased or decreased on a case-by-case basis if a different schedule is required by a customer's law or policy."

113. That language does not describe "the process the ALPR operator will utilize to determine if and when to destroy retained ALPR information." Instead, it delegates the retention decision entirely to Flock's customers, allowing retention periods to be "increased or decreased on a case-by-case basis" at the customer's discretion. SB 34 imposes the retention and destruction obligation on the ALPR *operator*—not the end user—and Flock cannot satisfy that obligation by deferring to whatever schedule its customers prefer.

114. For these reasons, Flock has collected, used, maintained, shared, and disseminated ALPR information without implementing or making public a policy that satisfies the minimum requirements of Civil Code section 1798.90.51, subdivision (b).

115. Flock's conduct was knowing, willful, and reckless. Flock was aware of SB 34's requirements and nonetheless collected and used ALPR information without a compliant policy. As detailed above, Flock markets its ALPR services to more than 200 California law enforcement agencies and holds itself out as a compliance partner for those agencies. The California Attorney General issued formal guidance in October 2023 explaining SB 34's policy requirements, including the obligation to implement a compliant usage and privacy policy that includes each of the disclosures enumerated in Civil Code section 1798.90.51, subdivision (b)(2). Flock's CEO acknowledged in August 2025 that the company was undertaking efforts to help users comply with applicable laws—an implicit admission that its prior practices did not ensure compliance. Despite this knowledge, Flock's posted LPR Policy has remained materially deficient, and Flock has continued to collect ALPR information from millions of California residents without a compliant policy. Flock's sustained failure to implement a compliant policy demonstrates knowing and reckless disregard for the statutory rights of Plaintiffs and Class Members.

116. Flock's failure to implement a compliant policy was compounded by its failure to maintain reasonable security procedures and adequate audit records, as alleged in the Third and Fourth Causes of Action. These failures are independently actionable but also demonstrate that

Flock's noncompliance with SB 34 was systemic—Flock did not merely fail to post the right words on its website, it failed to build any of the safeguards the statute requires.

117. Pursuant to Civil Code section 1798.90.54, Plaintiffs and Class Members are entitled to liquidated damages of $2,500 per violation, punitive damages, reasonable attorney's fees and litigation costs, and such other relief as the Court determines appropriate.

SECOND CAUSE OF ACTION
Violation of Civ. Code, § 1798.90.54, subd. (a)
(Unauthorized Access to and Use of California ALPR Information)
(By All Plaintiffs Against Defendant)

118. Plaintiffs incorporate the foregoing allegations as though fully set forth herein.

119. SB 34 prohibits California public agencies from sharing ALPR information with anyone other than another California public agency. (Civ. Code, § 1798.90.55, subd. (b).) Federal agencies and out-of-state law enforcement agencies are not "public agencies" under the statute. (See Civ. Code, § 1798.90.5, subd. (f).)

120. SB 34 independently requires ALPR operators to implement a usage and privacy policy that ensures "compliance with applicable privacy laws," Civil Code section 1798.90.51, subdivision (b)(2)(C), and to "[r]equire that ALPR information only be used for the authorized purposes described in the usage and privacy policy," Civil Code section 1798.90.52, subdivision (b).

121. Civil Code section 1798.90.54, subdivision (a) provides a right of action for the "unauthorized access or use of ALPR information," against "a person who knowingly caused the harm."

122. Flock knowingly caused harm to Plaintiff and Class Members by, *inter alia*: (a) designing their ALPR system to permit access to California ALPR data by federal agencies, out-of-state law enforcement agencies, and the public; (b) failing to implement technological safeguards to prevent unauthorized access; (c) failing to require that ALPR data be used only for authorized purposes; (d) failing to maintain reasonable security, resulting in the exposure of ALPR data through unprotected video feeds, compromised credentials, and improperly redacted audit reports; and (e) collecting and using Plaintiffs' and Class Members' ALPR data without

implementing an adequate, publicly available policy, thereby depriving them of their right to know which entities are collecting their data and how it is being used and maintained.

123. Flock's security and audit failures, as alleged in the Third and Fourth Causes of Action, further enabled and concealed the unauthorized sharing of California ALPR information. Flock's failure to require multifactor authentication facilitated credential sharing with unauthorized agencies. Its deficient audit records—which omitted required fields or recorded purposes only as "investigation"—made it impossible to detect, deter, or remedy unlawful access. These failures are independently actionable but also establish that Flock knowingly caused the unauthorized access and use of Plaintiffs' and Class Members' ALPR information.

124. Flock did not implement any policy or technical measure to prevent California ALPR information from being shared with federal agencies or out-of-state law enforcement agencies through its platform. Flock did not block such sharing, did not provide California agencies with the ability to restrict sharing to California public agencies as defined by SB 34, and did not require multifactor authentication or other reasonable access controls to prevent unauthorized users from searching California ALPR data.

125. Flock instead designed and configured its system—including its "National Lookup" and cross-jurisdictional sharing features—in a manner that permitted and facilitated the sharing of California ALPR information with federal agencies, including ICE, and out-of-state law enforcement agencies from multiple states.

126. Flock knew that its system permitted unlawful sharing. The California Attorney General issued formal guidance in October 2023 confirming that SB 34 does not permit sharing ALPR information with federal or out-of-state agencies. In February 2025, Flock itself notified California agencies that out-of-state agencies had been conducting broad searches of California ALPR data and conceded that those searches violated SB 34. Flock did not remove California from its national lookup system until mid-2025, and unlawful sharing continued even after that change.

127. On information and belief, Plaintiffs' and Class Members' ALPR information was actually accessed by federal agencies and out-of-state law enforcement agencies through Flock's

platform. In the alternative, Flock's system made Plaintiffs' and Class Members' ALPR information available for searching by any agency on its nationwide platform, including federal agencies and out-of-state law enforcement, without any technical restriction limiting access to California public agencies as defined by SB 34. By making California ALPR information accessible to unauthorized entities, Flock caused the "unauthorized access or use of ALPR information" within the meaning of Civil Code section 1798.90.54, subdivision (a).

128. Flock's conduct was knowing, willful, and reckless. Flock was aware of SB 34's requirements, was aware of the Attorney General's interpretation, and failed to implement reasonable measures to prevent the unlawful sharing of California ALPR information.

129. Plaintiffs and Class Members have been harmed by Flock's conduct. Their ALPR information was shared with federal agencies and out-of-state law enforcement agencies without their knowledge or consent, in violation of SB 34.

130. Pursuant to Civil Code section 1798.90.54, Plaintiffs and Class Members are entitled to liquidated damages of $2,500 per violation, punitive damages, reasonable attorney's fees and litigation costs, and such other relief as the Court determines appropriate.

THIRD CAUSE OF ACTION
Violation of Civ. Code, § 1798.90.51, subd. (a)
(Failure to Maintain Reasonable Security Procedures and Practices)
(By All Plaintiffs Against Defendant)

131. Plaintiffs incorporate the foregoing allegations as though fully set forth herein.

132. Civil Code section 1798.90.51, subdivision (a) requires ALPR operators to "[m]aintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure."

133. Flock failed to maintain reasonable security procedures and practices to protect Plaintiffs' and Class Members' ALPR information. As alleged herein, Flock's security failures include, but are not limited to: (a) failing to require multifactor authentication for users accessing its ALPR database; (b) maintaining hardware with critical physical vulnerabilities, including that pressing a button on the back of any publicly mounted Flock camera grants root access to the

device; (c) operating its cameras on Android Things 8.1, a discontinued Google operating system that no longer receives security patches; (d) making internal testing data accessible online; (e) permitting live video feeds from its "Condor" cameras, including cameras in California, to be viewed on the internet without any authentication; and (f) failing to implement reasonable technical controls to prevent federal agencies and out-of-state law enforcement from accessing California ALPR information through its cross-jurisdictional sharing features.

134. These security failures exposed Plaintiffs' and Class Members' ALPR information to unauthorized access, including by federal agencies and out-of-state law enforcement.

135. Flock's security failures independently constitute a "breach of security of an ALPR system" and have resulted in the "unauthorized access or use of ALPR information" within the meaning of Civil Code section 1798.90.54, subdivision (a). Even apart from any actual breach, Flock's failure to maintain reasonable security procedures and practices is itself a violation of Civil Code section 1798.90.51, subdivision (a) that has harmed Plaintiffs and Class Members by leaving their ALPR information without the protections the Legislature required.

136. Flock's conduct was knowing, willful, and reckless. Flock was aware of SB 34's security requirements, was aware of the vulnerabilities in its system, and failed to implement reasonable safeguards.

137. Pursuant to Civil Code section 1798.90.54, Plaintiffs and Class Members are entitled to liquidated damages of $2,500 per violation, punitive damages, reasonable attorney's fees and litigation costs, and such other relief as the Court determines appropriate.

FOURTH CAUSE OF ACTION
Violation of Civ. Code, § 1798.90.52
(Failure to Maintain Adequate Audit Records and Ensure Authorized Use)
(By All Plaintiffs Against Defendant)

138. Plaintiffs incorporate the foregoing allegations as though fully set forth herein.

139. Civil Code section 1798.90.52, subdivision (a) requires ALPR operators that access or provide access to ALPR information to "[m]aintain a record of that access," including "[t]he date and time" of access, "[t]he license plate number or other data" that was queried, "[t]he username of the person who accesse[d] the information," and "[t]he purpose of the access."

140. Civil Code section 1798.90.52, subdivision (b) requires ALPR operators to "[r]equire that ALPR information only be used for the authorized purposes described in the usage and privacy policy."

141. Flock failed to maintain audit records sufficient to satisfy Civil Code section 1798.90.52, subdivision (a). As alleged herein, Flock's audit reports—which are routinely obtained through public records requests—exposed hundreds of thousands of unredacted license plate numbers alongside the reasons officers searched for them. Rather than implementing reasonable redaction and access controls, Flock stripped officer names and license plate numbers from its audit reports entirely, rendering them insufficient for the oversight SB 34 requires. An audit record that omits the identity of the user or the data queried does not satisfy the statute.

142. Flock also failed to maintain audit records that meaningfully document "[t]he purpose" of the access as required by section 1798.90.52(a)(4). Public reporting and audit materials reflect widespread searches with no case number and no stated reason beyond generic labels such as "investigation." Records that use non-descriptive placeholders for the purpose of access defeat the auditability SB 34 mandates and undermine the Legislature's intent that ALPR access be meaningfully reviewable and accountable.

143. Flock further failed to require that ALPR information be used only for authorized purposes as required by section 1798.90.52, subdivision (b). Flock's system permitted and facilitated the use of California ALPR information by federal agencies and out-of-state law enforcement agencies—uses that are not authorized under SB 34. Audit logs and public reporting have documented uses that include discriminatory search terms and cross-border investigations related to abortion and other sensitive medical care.

144. These audit and proper-use failures independently harmed Plaintiffs and Class Members by depriving them of the statutory protections designed to ensure that access to their ALPR information is transparent, accountable, and limited to authorized purposes. The failures also enabled and concealed the unauthorized sharing of California ALPR information with federal and out-of-state agencies.

145. Flock's conduct was knowing, willful, and reckless. Flock was aware of SB 34's

audit and proper-use requirements, was aware that its audit records were deficient, and failed to take adequate corrective action.

146. Pursuant to Civil Code section 1798.90.54, Plaintiffs and Class Members are entitled to liquidated damages of $2,500 per violation, punitive damages, reasonable attorney's fees and litigation costs, and such other relief as the Court determines appropriate.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, pray for judgment against Defendant as follows:

(a) An order certifying the Class as defined herein and appointing Plaintiffs as Class Representative and Plaintiffs' attorneys as Class Counsel;

(b) An order declaring that Defendant's conduct violates Civil Code sections 1798.90.5 through 1798.90.55;

(c) Compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury, but not less than $2,500 per violation of Civil Code section 1798.90.54;

(d) Prejudgment interest on all amounts awarded;

(e) Punitive and exemplary damages;

(f) Restitution and disgorgement of all ill-gotten gains;

(g) Injunctive relief requiring Defendant to: (i) cease all unlawful sharing of California ALPR data; (ii) implement and maintain reasonable security practices in compliance with the ALPR Law; (iii) implement and maintain safeguards preventing the sharing of California ALPR data with federal and out-of-state agencies; and (iv) implement and maintain a compliant usage and privacy policy;

(h) Reasonable attorneys' fees, expenses, and costs of suit, including under Code of Civil Procedure section 1021.5;

(i) Such other and further relief as the Court deems just and proper.

JURY TRIAL

Plaintiffs demand a trial by jury for all issues so triable.

Respectfully submitted,

DORIAN ELDRIDGE and SILAS PEREZ, individually and on behalf of all others similarly situated,

Dated: February 18, 2026

By: /s/ *J. Aaron Lawson*

J. Aaron Lawson (SBN 319306)
alawson@edelson.com
Mickey Terlep (SBN 367340)
mterlep@edelson.com
EDELSON PC
150 California Street, 18th Floor
San Francisco, California 94111
Tel: (415) 212-9300

Counsel for Plaintiffs and the Putative Class