

# Congress of the United States

Washington, DC 20515

November 3, 2025

The Honorable Andrew N. Ferguson  
Federal Trade Commission  
600 Pennsylvania Avenue, NW  
Washington, D.C. 20580

Dear Chair Ferguson:

We write to request that the Federal Trade Commission (FTC) investigate Flock Safety (“Flock”), the license plate surveillance camera company, and, where appropriate, hold the company responsible for its negligent cybersecurity practices. Flock’s surveillance data can reveal Americans’ movements over time, including trips to doctors and therapists, support group meetings for alcohol or drug addiction, as well as places of worship and protests. By not requiring industry-standard multi-factor authentication (MFA) to secure law enforcement accounts, Flock has needlessly exposed Americans’ sensitive personal data captured by the company’s surveillance cameras to theft by hackers and foreign spies, and unauthorized access through multiple documented instances of unauthorized password sharing.

Flock operates the largest network of surveillance cameras in the United States, reportedly contracting with over 5,000 police departments, 1,000 businesses, and numerous homeowners associations across 49 states. When a vehicle passes by a Flock camera, Flock records plate information, vehicle characteristics, and when and where the vehicle was spotted. Flock’s network of surveillance cameras generate and store billions of vehicle scans each month. Flock reportedly enables law enforcement to search through this data not just by plate number, but also by make, model, and even bumper stickers.

In addition to being able to search data generated by cameras their agencies pay for, Flock’s law enforcement customers can also search data collected by other Flock customers’ cameras. Flock customers can allow access by specific law enforcement agencies and can also enroll into the “National Lookup Tool” which allows their data to be searched by all other enrolled Flock customers. Flock informed Congress this August that approximately 75% of Flock’s law enforcement customers have opted into the National Lookup Tool, which is likely due to Flock restricting access to nationwide searches to agencies that have agreed to share their data. But because most law enforcement agency customers have access to this tool, hackers, foreign spies, or anyone else that gains access to a Flock customer account can misuse it to track Americans across the country.

Flock has unnecessarily exposed Americans’ sensitive personal data to theft by hackers and foreign spies. While Flock offers support for MFA, a widely recognized cybersecurity best practice, Flock does not require it, which the company confirmed to Congress in October. Moreover, Flock continues to support insecure methods of MFA, such as sending a numeric code to a phone by text message, which is vulnerable to interception and phishing. Flock does not natively support phishing-resistant MFA, which the Cybersecurity and Infrastructure Security Agency calls “the gold standard method of [MFA].” Phishing-resistant MFA is required of federal agencies and mandated by both the Federal Communications Commission and the FTC

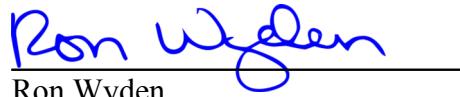
Flock's failure to natively support and require phishing-resistant MFA means that if hackers or foreign spies steal, phish, or otherwise learn a law enforcement officer's Flock password, they can gain access to law-enforcement-only areas of Flock's website and search the billions of photos of Americans' license plates collected by taxpayer-funded cameras across the country. This threat is not theoretical. A search by Congressional staff of a public tool operated by the cybersecurity company Hudson Rock documenting accounts compromised by a form of malware known as an "infostealer" reveals that passwords for at least 35 Flock customer accounts have been stolen. Security researcher Benn Jordan also recently provided our offices with a screenshot from a Russian-language cybercrime forum in which Flock accounts appear to be offered for sale.

By not requiring MFA, Flock has also enabled unauthorized access through law enforcement officers sharing their Flock passwords. If Flock required MFA, law enforcement users of Flock would be required to approve each login to their account from a new computer. On August 11, 2025, Unraveled Press revealed that a Drug Enforcement Administration officer used the Flock account of a local police detective in Palos Heights, Illinois, to conduct several searches. Public records obtained by the press revealed that the detective confirmed that it was a common practice for members of a DEA task force that he was part of to use his login credentials to conduct Flock searches. That numerous federal agents were able to access Flock's systems using passwords belonging to other users without being detected or blocked raises serious questions about the effectiveness of Flock's cybersecurity defenses. A July 9, 2025, memo by the Palos Heights Deputy Chief of Police about the incident, which was released to the press, revealed that the department had not enabled the MFA option until after the password sharing was first identified by a reporter at 404 Media.

Flock's failure to require MFA is likely an unfair business practice prohibited by Section 5 of the FTC Act. In at least four cases — against Uber, Chegg, Drizly, and Blackbaud — the FTC held that failure to require MFA is an unfair business practice. Flock's negligent cybersecurity practices may also violate state laws related to data protection, consumer privacy or the use of automatic license plate reader (ALPR) systems; for example, California Civil Code § 1798.90.53 requires entities operating ALPR systems to "maintain reasonable security procedures and practices, including operational, administrative, technical, and physical safeguards, to protect ALPR information from unauthorized access, destruction, use, modification, or disclosure."

Flock has received vast sums of taxpayer money to build a national surveillance network. But Flock's cavalier attitude towards cybersecurity needlessly exposes Americans to the threat of hackers and foreign spies tapping this data. Accordingly, we urge the FTC to hold Flock accountable for its negligent cybersecurity practices.

Sincerely,

  
Ron Wyden  
United States Senator

  
Raja Krishnamoorthi  
Member of Congress