



HOUSE OF DELEGATES WEST VIRGINIA LEGISLATURE

August 14, 2026

Chief Executive Officer Garrett Langley
Flock Safety
3284 Northside Parkway NW
Atlanta, GA 30327

Mr. Langley:

Yesterday you published a blog post on the Flock Safety website entitled “Flock Updates Privacy, Accountability, Security, and Transparency Safeguards.”¹ The blog post announced: “At the beginning of this month, we also made multi-factor authentication (MFA) mandatory for anyone logging into Flock, increasing our security standards for all customers.” Yet this announcement contradicts sworn testimony the Flock Safety Director of Government Affairs Kevin Kane provided to the West Virginia Legislature just five days ago that two-factor authentication has been required “for a long time.”

Mr. Kane provided this testimony on August 9, 2026, at a meeting of the Joint Standing Committee on Government Organization in the House of Delegates chamber at the West Virginia Capitol building in Charleston, West Virginia. Mr. Kane had been asked to provide a presentation on the topic, “What are local governments contracting for when they purchase Flock Cameras and automated license plate reader (ALPR) equipment and services?” He was administered an oath at the beginning of the hearing requiring him to provide truthful testimony.

In his opening statement, Mr. Kane testified: “I want to be very clear that Flock Safety has never been hacked.” Mr. Kane subsequently had the following exchange with Delegate Patrick Lucas, whose legislative district includes the City of Huntington, West Virginia, which recently concluded a contract with Flock Safety:

DEL. LUCAS: You can’t get on any social media without a lot of people saying certain things about it. So let me ask you a few questions. You said during your testimony that Flock Safety has never been hacked.

MR. KANE: Yes, sir, that’s correct.

DEL. LUCAS: And that’s good information. I’m glad to hear that, because there’s information out there saying differently. So I guess my question to you is, can Flock Safety be hacked?

¹ <https://www.flocksafety.com/blog/flock-guardrails-address-lpr-privacy-concerns-and-police-transparency>.

MR. KANE: I think any system is capable of being hacked I would say in regard to that, this is exactly why we do things like provide two-factor authentication. This is exactly why we ensure data is secured end to end. This is exactly why we have the types of certifications to ensure that we have the industry leading practices to protect citizen data.

After Delegate Lucas, Delegate Ryan Browning was recognized for questions. Mr. Kane had this exchange with Delegate Browning, whose district is also near Huntington, West Virginia:

DEL. BROWNING: Do you guys require two-factor authentication to log into the system?

MR. KANE: Yes.

DEL. BROWNING: Is that recent?

MR. KANE: It's been a standard practice for a long time. I'm not sure exactly how long, but it's I've been with the company for three years and it's been there for a long time.

After Delegate Browning, Delegate Tristan Leavitt was recognized for questions. Mr. Kane had the following exchange with Delegate Leavitt:

DEL. LEAVITT: I want to start with just a couple of the colloquies you just had with some of my colleagues. One of them was about never having been hacked. Can you just repeat that claim again?

MR. KANE: Yes, sir. There are some videos on YouTube that purport to have hacked Flock. At no point in time did those videos or that individual ever gain access to Flock's database.

DEL. LEAVITT: So did they gain access to the video footage?

MR. KANE: Due to a bug, for a very limited number of cameras for a very brief period of time, yes. But that did not give access to the system.

DEL. LEAVITT: So how many incidents have there been where raw video footage has been accessed from outside of authorized users in Flock products?

MR. KANE: I'm not aware of any other.

Mr. Kane purported to be unaware of one media outlet reporting it had been able to access 60 cameras in Bakersfield, California.² Delegate Leavitt subsequently had this exchange with Mr. Kane:

DEL. LEAVITT: There's been a lot of reporting that two-factor authentication is not required by the local departments. You say you guys have used two-factor authentication for a long time.

MR. KANE: You're talking about at the corporate level or are you saying your customers?

DEL. LEAVITT: I'm saying at the customer level. So you don't know when that requirement was put into place?

MR. KANE: It originally started out when I joined the company as a potential optional feature because some police departments told us that they do not have the ability to due to cell access or whatever reason, that two-factor would not work. It has always been an optional feature and we've made that mandatory. I think that's been done within the last year.

It was already concerning to see Mr. Kane shift his testimony from implying two-factor authentication had been required for as long as three years to testifying it was adopted "within the last year." Now, your blog post has revealed multi-factor authentication was made mandatory literally only days before our hearing.

We are legislators who have strong relationships with law enforcement in our communities, and understand that robust policing is essential to keeping the public safe. We recognize the need for tools to aid in difficult law enforcement challenges like finding missing persons and stopping drug traffickers—the latter particularly relevant here in West Virginia, which has had the highest annual opioid *and* drug overdose deaths for 15 consecutive years.³

Yet state legislatures also have the responsibility to adopt responsible safeguards for their state. We will be considering—if not introducing—relevant legislation in our 2027 legislative session. Some have already proposed a ban on government-operated ALPRs. Legislating in this area is incredibly difficult to do for an emerging and often evolving area of technology if witnesses before government bodies do not provide accurate testimony.

Unfortunately, this week's hearing is not the first time government officials have felt misled by Flock Safety. In 2021, a Flock Safety representative reportedly told the Urbana,

² <https://www.404media.co/flock-exposed-its-ai-powered-cameras-to-the-internet-we-tracked-ourselves>. The day after this report Flock published a blog post entitled: "Update on Limited Condor Device Configuration Issue." <https://www.flocksafety.com/blog/update-on-limited-condor-device-configuration-issue>. Two weeks later, Flock released a blog post with the title "Has Flock Been Hacked?" and the subtitle: "No, Flock has never been hacked, and there has not been a leak of Flock information." <https://www.flocksafety.com/blog/has-flock-been-hacked>.

³ <https://www.cdc.gov/nchs/products/databriefs/db294.htm>; <https://usafacts.org/answers/how-many-drug-overdose-deaths-happen-every-year-in-the-us/state/west-virginia>; <https://www.kff.org/mental-health/opioid-overdose-deaths-national-trends-and-variation-by-demographics-and-states>.

Illinois city council that Flock had “worked with groups like the ACLU to design an ALPR system that takes considerations they have into account”—only to have that claim soundly repudiated by the ACLU.⁴

In August 2025, Flock Safety reportedly reassured Loveland, Colorado Police Chief Tim Doran federal agencies did not have access to Loveland’s ALPRs; after a local news station released an expose based on public records requests,⁵ you admitted in an August 25, 2025 blog post: “[S]ome of our public statements inadvertently provided inaccurate information.”⁶

On March 4, 2026, Mr. Kane reportedly testified before the Connecticut General Assembly’s General Law Committee that Flock has never had a data-sharing request come in from a federal agency.⁷ Yet your own aforementioned August 2025 blog post read: “While it is true that Flock does not presently have a contractual relationship with any U.S. Department of Homeland Security agencies, we have engaged in limited pilots with the U.S. Customs and Border Protection (CBP) and Homeland Security Investigations (HSI), to assist those agencies in combatting human trafficking and fentanyl distribution.”⁸

On April 21, 2026, upon reassurance from a Flock Safety representative that Flock’s license plate readers did not create heat maps to track vehicles, the Oshkosh, Wisconsin city council voted to renew a contract with Flock Safety. Less than twenty-four hours later, law enforcement in that city came to believe Flock Safety had provided false information regarding heat maps, and the city council voted unanimously to rescind their vote of the previous evening.⁹

Given this recent history, and the public stakes involved in these issues, Mr. Kane might have been expected to be fully prepared to answer questions before our legislature candidly, completely, and most of all, truthfully. Indeed, given that Flock Safety is valued at \$8.4 billion dollars and has the lion’s share of the market in this technology, your company has the resources to provide impeccable communication with lawmakers and with the public. Instead, Flock Safety’s history of providing inaccurate information is quite frankly unacceptable.

Accordingly, as soon as possible, but no later than September 1, 2026, please provide the following information, much of which we requested in our August 9, 2026 hearing:

I. Security Incidents & Unauthorized Access

1. For each year since Flock Safety’s founding and for each Flock Safety product line, how many incidents is Flock Safety aware of where raw video footage has been accessed by unauthorized users?

⁴ <https://www.aclu.org/news/privacy-technology/tracking-alpr-cameras/flock-safety-credibility-lost-as-it-repeatedly-lies-to-city-councils-police-departments-and-public-across-the-country>.

⁵ <https://www.9news.com/article/news/local/flock-federal-immigration-agents-access-tracking-data/73-a8aee742-56d4-4a57-b5bb-0373286dfef8>.

⁶ <https://www.flocksafety.com/blog/ensuring-local-compliance>.

⁷ <https://ctnewsjunkie.com/2026/03/05/flock-safety-official-testifies-in-favor-of-cts-privacy-bill>.

⁸ <https://www.flocksafety.com/blog/ensuring-local-compliance>.

⁹ <https://www.wbay.com/2026/04/23/oshkosh-council-rescinds-flock-camera-contract-after-false-statements>.

2. What investigations did Flock Safety conduct of each instance of unauthorized access?
3. For each instance of unauthorized access, what was the cause of the security breach?
4. What remedial steps has Flock Safety taken after each security breach to prevent recurrence?

II. Surveillance Scope & Data Sharing

5. Please reconcile Mr. Kane's March 4, 2026 claim with the August 25, 2025 blog post regarding pilot programs with CBP and HSI.
6. Were the CBP and HSI pilots requested by those agencies, or by Flock Safety?
7. Which Flock Safety product lines feed the National Lookup Tool available for license plate data?
8. What percentage of Flock Safety automated license plate reader users are currently opted into the National Lookup Tool?
9. Is there an equivalent of the National Lookup Tool for Flock Safety Condor cameras?
10. Will Flock Safety's Condor camera return FreeForm natural language search results for such bodily characteristics as height, hair color, wearing glasses, or a scar on one's face?

III. Accuracy & False Positive Rates

11. For each year since Flock Safety's founding, how many false "Hot List" positives have been generated by:
 - a. Flock Safety's Falcon license plate reader; and
 - b. Flock Safety's Sparrow license plate reader.
12. Based on the aforementioned false positive data, what was the accuracy rate of the Falcon license plate reader for all license plate "Hot List" hits in 2025?
13. Based on the aforementioned false positive data, what was the accuracy rate of the Sparrow license plate reader for all license plate "Hot List" hits in 2025?

IV. Internal Oversight & Employee Access Controls

14. For each corporate division of Flock Safety, approximately how many employees have access to all customer data?
15. How often does Flock Safety audit its employees' access of customer data? What do the audits consist of? Do such audits comprehensively review every search, or only perform spot checks?

16. Since Flock Safety's founding, how many employees have ever been found to have improperly accessed customer data?

V. Data Governance & Infrastructure

15. What disaster recovery backup methods does Flock Safety use for customer data?

16. How are metadata, derivative data, analytics, insights, intelligence, and extracted data from footage governed across Flock Safety's platforms? Who owns the aforementioned?

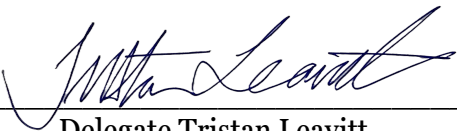
17. How long are metadata, derivative data, analytics, insights, intelligence, and extracted data from customer products retained by Flock Safety for research purposes?

18. Please list all contracts Flock Safety has ever had with entities outside of the United States to conduct third-party review of Flock Safety data, metadata, derivative data, analytics, insights, intelligence, or extracted data.

19. Please provide your most recent SOC 2 Type II compliance audit.

Thank you in advance for your prompt cooperation in this matter.

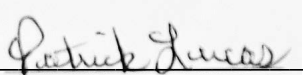
Cordially,



Delegate Tristan Leavitt



Delegate Ryan Browning



Delegate Patrick Lucas

cc: Kevin Kane, Flock Safety
Chairman Chris Phillips, West Virginia House Committee on Government Organization
Chairman JB Akers, West Virginia House Committee on the Judiciary
Speaker Roger Hanshaw, West Virginia House of Delegates
President Randy Smith, West Virginia Senate