



HOUSE OF DELEGATES WEST VIRGINIA LEGISLATURE

October 12, 2026

Dan Haley, Chief Legal Officer
Flock Safety
3284 Northside Parkway NW
Atlanta, GA 30327

Mr. Haley:

Your letter of October 9, 2026, begins with the claim that Flock Safety did not intend to suggest “off the record” discussions “behind closed doors.” In our August 9, 2026, public proceeding with Flock Director of Government Affairs Kevin Kane, he stated on multiple occasions his desire to follow up with lawmakers individually, including by saying:

- “I’m happy to follow up with you *in your office* to ensure that I provide you with the accurate answer that you deserve.”¹
- “I think it would probably helpful if I can follow up with you *in your office* and our security team to provide more insight in terms of specifically how that’s conducted.”²

Given that we were unable to obtain significant facts in our public forum, we sent a letter so there would be a written record of Flock’s responses. In reply, your September 1, 2026, letter read: “[M]y team would welcome the chance to provide a briefing to the Committee, including appropriate technical personnel, to walk through any of the matters above[.]” It was transmitted to us with an email which stated: “Once you’ve had a chance to review, please let us know if you or any of your colleagues would like to discuss further[.]” And once again, your September 16, 2026, letter—sent the same day as significant reporting about new breaches of video footage³—read: “To avoid any further misunderstandings, we believe it would be beneficial to meet with you again. We would welcome the opportunity to sit down together to discuss your remaining questions and review our answers directly.”

“Briefing[s],” “discuss[ing] further,” and “sitt[ing] down together” are not ways this Committee would typically characterize public proceedings. Given that you have still failed to provide in your letters information such as how many employees have ever been found to have improperly accessed customer data, what “non-U.S. vendor” Flock Safety sends customer images to, and false positive data prior to July 2026 for license plate readers, please forgive our strong impression that Flock Safety was avoiding putting this information on the record.

¹ 1:12:48 mark in hearing.

² 1:15:53 mark in hearing.

³ <https://www.wired.com/story/hackers-flock-camera-data-shows-how-system-works>;
<https://www.404media.co/hackers-stole-flocks-camera-software-revealing-how-the-company-tracks-cars-and-people-2>.

In light of your commitment to meet at our convenience for an on-the-record briefing to the Committee, please plan for Flock Safety to testify under oath at our next public meeting, November 9, 2026, at 2 pm at the West Virginia Capitol. Flock Safety should provide sufficiently knowledgeable witnesses to provide full answers to the following questions.

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?**

You indicated in your October 9 letter that Flock has only experienced a single incident where camera streams were exposed to the public internet. However, our letter asked about video *footage* being accessed by unauthorized users, not just video streams. On September 16, 2026—the same day as your letter inviting us to “sit down together to discuss your remaining questions”—*Wired* and *404 Media* published concurrent stories regarding a hacking collective cutting down a Flock camera, accessing the encryption key stored on the device, and unlocking more than 27,000 videos.⁴ On September 24, 2026, Flock Safety published an update on its Security Center reading:

Flock is aware of a news article that makes claims regarding vulnerabilities in our legacy Falcon LPR. The device in question was stolen from a law enforcement customer. Flock is not able to verify claims regarding data on the device. Flock was able to confirm, however, that the device was susceptible to a vulnerability that was flagged in a finding from our 2026 annual penetration test.⁵

Your witness(es) should explain:

- Whether this device was contemporaneously reported to Flock as stolen;
- Whether Flock rotated or revoked this device's cloud credentials once it was reported missing;
- When the fix for this issue reached devices;
- Whether the September 24, 2026, Security Alert was referencing this incident or another incident;
- Whether other exfiltrations of “proprietary and confidential information belonging to Flock Safety and its customers” are *alleged* to have occurred even if Flock has not been able to verify the claims;
- Whether any of the vulnerabilities identified by Bishop Fox or otherwise brought to Flock's attention could have resulted Flock data or Flock customer data being accessed, and what those vulnerabilities or alleged exfiltrations consisted of;
- Why Flock Safety's October 9 letter to us did not disclose the accessing of video footage described in the September 16, 2026, reporting; and
- To the extent Flock believes this exfiltration of footage was not covered by the question in our August 14, 2026, letter, what other similar incidents have

⁴ <https://www.wired.com/story/hackers-flock-camera-data-shows-how-system-works;>
[https://www.404media.co/hackers-stole-flocks-camera-software-revealing-how-the-company-tracks-cars-and-people-2.](https://www.404media.co/hackers-stole-flocks-camera-software-revealing-how-the-company-tracks-cars-and-people-2)

⁵ [https://security.flocksafety.com?tcuUid=45857a70-9d00-4e39-b91d-9faf38a86b15.](https://security.flocksafety.com?tcuUid=45857a70-9d00-4e39-b91d-9faf38a86b15)

occurred that Flock does not believe were previously necessary to disclose in response to that letter.

The question in our initial letter focused on video footage being accessed by unauthorized users because Mr. Kane repeatedly told our legislature that Flock Safety had “never been hacked” before being forced to acknowledge that unauthorized users had been able to access Flock devices, with both their live streams and their archived data. On September 22, 2026, in a brief description of a penetration test by cybersecurity firm Bishop Fox, Flock wrote: “None of these findings resulted in any customer data or systems being accessed by anyone outside Flock.”⁶

Yet on September 23, 2026, Joshua Michael published the website <https://flocksurveillance.org>, which included the location of 300,000 Flock surveillance devices across the United States. The next day, *The Intercept* published a story regarding how Michael discovered Flock’s servers were “publicly leaking data in the form of an access token that could be acquired without needing to log in. With that token, . . . he could query ArcGIS, a third-party geographic information system platform used by Flock, to retrieve the locations of Flock devices.”⁷ He reportedly notified Flock of the issue several times in November 2025, but received no response other than a stock two-sentence email after his third attempt.⁸ He also published his findings in an extensive blog post in January 2026.⁹

Flock Safety notified its customers that an “exposed map access key” from a “third party map service” was used to unlawfully access and exfiltrate data, and on September 25, 2026, Flock reportedly sent the individual who exfiltrated the data a letter demanding he take down his website based on it, describing the data as “proprietary and confidential information belonging to Flock and its customers.”¹⁰

Thus, your witness(es) should also explain whether Flock is aware of *any* other unauthorized access or exfiltration of any Flock data or Flock customer data, regardless of whether from a Flock device, a Flock server, or any other third-party means.

2. What investigations did Flock Safety conduct of each instance of unauthorized access?

Your witness(es) should particularly explain what investigation Flock Safety conducted of the vulnerabilities outlined in the September 16 reporting.

3. For each instance of unauthorized access, what was the cause of the security breach?

Your witness(es) should explain what “isolated security risks” Flock has observed not stemming from “customer-side issues”, and particularly what investigation Flock Safety conducted of the vulnerabilities identified in the September 16, 2026, *Wired* and *404 Media* stories.

⁶ <https://www.flocksafety.com/blog/flock-security-testing-2026-what-the-bishop-fox-penetration-test-found>.

⁷ <https://theintercept.com/2026/09/24/how-many-flock-devices-in-united-states-300000>.

⁸ *Id.*

⁹ <https://nexanet.ai/blog/53-times-flocksafety-hardcoded-the-password-for-americas-surveillance-infrastructure>.

¹⁰ <https://footnote4a.org/news/bishop-fox-3>.

4. What remedial steps has Flock Safety taken after each security breach to prevent recurrence?

Your witness(es) should explain what steps Flock Safety took after the August 9, 2026, Gainsec report, and the September 16, 2026, *Wired* and *404 Media* reporting, as well as whether Flock continues to store encryption keys on local devices or has begun encrypting the entire contents of devices.

II. Surveillance Scope & Data Sharing

6. Were the CBP and HSI pilots requested by those agencies, or by Flock Safety?

If Flock Safety is “unable to determine whether these particular pilots were prompted by an incoming request or a proactive offer,” as you write, your witness(es) should be prepared to explain how this legislature can trust Flock Safety when it makes a claim such as that Flock has never had a data sharing-request come in from a federal agency.

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.

As we reiterated in our September 3, 2026, letter, these questions require that your witness(es) provide inaccuracy data for 2017-2025, by year, not your “most up-to-date hotlist accuracy numbers in 2026.” Understanding that Sparrow is a name Flock no longer uses for its license plate readers, your witness(es) may provide consolidated numbers (by year) for all Flock license plate reader models.

As discussed with Mr. Kane, your witness(es) should also detail how inaccuracies are reported and recorded, and whether there is a system for reporting false positives in real-time or whether this number is based on “surveys and things like that with customers,” as Mr. Kane previously testified.

12/13. Based on the aforementioned false positive data, what was the accuracy rate of the Falcon/Sparrow license plate reader for all license plate “Hot List” hits in 2025?

Your witness(es) should explain how optical character recognition (OCR) and license plate accuracy are measured, such as per character, per plate, or per overall scan?

IV. Internal Oversight & Employee Access Controls

14. For each corporate division of Flock Safety, approximately how many employees have access to all customer data?

Your letter states: “No corporate division or employee possesses broad, unrestricted access to all customer data.” Your letter provided no definition of the word “unrestricted.” Your letters have made clear that Flock Safety does not conduct

comprehensive audits to determine whether Flock employees conduct customer searches for personal or investigative purposes, leaving the word “unrestricted” uselessly vague.

Therefore, your witness(es) should be sufficiently knowledgeable and prepared to answer the following:

- What level of employee access is required in order to view live customer feeds, as Flock Safety’s Director of Growth did with the Dunwoody, Georgia contract 181 times in 2025, Flock’s Vice President of Strategic Relations and Business Development did with the Dunwoody, Georgia contract 163 times in 2025 (including of the Marcus Jewish Community Center of Atlanta’s gymnastics room), a Principal Product Manager did with the Dunwoody, Georgia contract 81 times in 2025, and a Business Development Manager did with the Dunwoody, Georgia contract 54 times in 2025?¹¹
 - For each corporate division of Flock Safety, approximately how many employees have this level of access?
- What level of employee access is required in order to view recorded customer footage, as Flock Safety’s Vice President of Strategic Relations and Business Development did with the Dunwoody, Georgia contract 22 times in 2025 and a Flock Engineer did with the Dunwoody, Georgia contract 21 times in 2025?¹²
 - For each corporate division of Flock Safety, approximately how many employees have this level of access?
- Does Flock Safety require any higher level of employee access to view live feeds or recorded footage of areas with high usage by minors, as Flock Safety’s Vice President of Strategic Relations and Business Development did with the Dunwoody, Georgia Brook Run playground repeatedly?¹³
 - For each corporate division of Flock Safety, approximately how many employees have this level of access?
- What level of employee access is required in order to disable the multi-factor authentication requirement for a user, as a Flock Safety employee did with the Dunwoody, Georgia contract on September 9, 2025?¹⁴
 - Did the level of access necessary to disable the multi-factor authentication requirement for a user change when Flock made multi-factor authentication mandatory at the beginning of August 2026?
 - For each corporate division of Flock Safety, approximately how many employees have this level of access?

¹¹ <https://jasonhunyar.substack.com/p/why-are-flock-employees-watching-720>.

¹² *Id.*

¹³ <https://jasonhunyar.substack.com/p/flock-vp-watched-recordings-from>.

¹⁴ <https://jasonhunyar.substack.com/p/why-are-flock-employees-watching-720>.

- What level of employee access is required in order to disable a user's searches showing up in audits, as a Flock Safety employee did with the Dunwoody, Georgia contract on September 9, 2025?¹⁵
 - For each corporate division of Flock Safety, approximately how many employees have this level of access?
- What level of employee access is required in order to create local users who do not show up in user logs, as a Flock Safety employee did with the Dunwoody, Georgia contract on November 2, 2025?¹⁶
 - For each corporate division of Flock Safety, approximately how many employees have this level of access?
- What level of employee access is required in order to create APIs of customer data to third-party companies, as a Flock Safety employee did with the Dunwoody, Georgia contract on January 28, 2025?¹⁷
 - For each corporate division of Flock Safety, approximately how many employees have this level of access?
- For each corporate division of Flock Safety, approximately how many employees have access to any form of elevated technical access?
- For each corporate division of Flock Safety, how many employees have access to perform backup restoration?

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?

Your witness(es) should explain why Flock Safety does not conduct scheduled audits of all employee queries, since Flock's own witness testified before our legislature on August 9, 2026, that conducting regular audits is essential and "just . . . relying upon the technology" was insufficient to prevent abuse.

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

Your letters have made no attempt whatsoever to answer this question. Your witness(es) should answer this question in detail, including how many employees have ever been found to have accessed data outside authorized technical duties, how many have experienced any form of access revocation or reduction, how many have experienced personnel sanctions for such conduct, and how many have been terminated for such conduct.

¹⁵ *Id.*

¹⁶ *Id.*

¹⁷ *Id.*

V. Data Governance & Infrastructure

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

Your October 9, 2026, letter states “non-U.S. vendors exclusively for machine-learning data annotation to improve model accuracy across varying weather and lighting conditions. . . . Annotators work solely on isolated, decontextualized images stripped of customer identifying metadata.” This question was about all forms of data, not simply “customer identifying metadata.” Your witness(es) should be prepared to answer questions on this issue in detail, including what it means that “[i]mages . . . are separated from the customer environment,” whether vehicle license plates included in these images, and how Flock Safety can claim “[c]ustomers retain full ownership and control over all customer data” when some subset of images is sent outside of the United States by Flock Safety.

Finally, your witness(es) should answer the question Delegate Kayla Young asked Mr. Kane which he said he would “follow up” on: what data restrictions exist on data sent out of the country.

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

Again, your October 9, 2026, letter states “non-U.S. vendors exclusively for machine-learning data annotation to improve model accuracy across varying weather and lighting conditions. . . . Annotators work solely on isolated, decontextualized images stripped of customer identifying metadata.” Your witness(es) should explain whether Flock Safety has a retention policy for these images, what Flock's retention period is for them, whether the non-U.S. vendors have a retention policy for these images, what the vendor retention period is for them, what oversight Flock conducts to ensure the vendors are adhering to the retention period, and why Flock specifically excludes images from states with a statutory license plate reader data retention period.

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.

Your witness(es) should provide the name, country, and precise location of the “non-U.S. vendor” referenced in your September 1, 2026, letter, explain what vetting Flock subjects this vendor and its employees to, explain what functions Flock Safety's wholly-owned subsidiary in Finland performs, and explain whether that subsidiary has any access whatsoever to any U.S.-originating data.

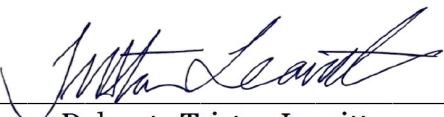
19. Please provide your most recent SOC 2 Type II compliance audit.

We have requested access at security.flocksafety.com to the SOC 2 report and the penetration test (“pentest”) report completed by Bishop Fox. Your witness(es) should be prepared to explain what two “critical” level vulnerabilities Bishop Fox found with Flock's cloud infrastructure, what six “high” level vulnerabilities it found, what Flock has

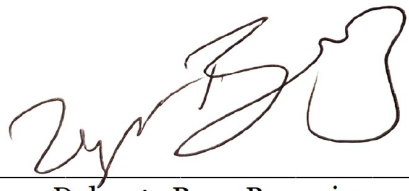
done to remedy those vulnerabilities, why Flock has not updated its common vulnerabilities and exposures (CVE) entries since late 2025,¹⁸ when Flock will publish CVE records and fix information for the 2025 and 2026 findings now that it has been authorized as a CVE Numbering Authority (CNA),¹⁹ whether the encryption on Flock's devices uses FIPS 140-validated modules (with certificate numbers), which National Institute of Standards and Technology (NIST) frameworks Flock is formally assessed against and by whom, and Flock's exact current FedRAMP status.

Please confirm by Monday, October 19, 2026, that Flock Safety will appear on November 9, 2026, and please provide the names of Flock's proposed witness(es) by October 26, 2026.

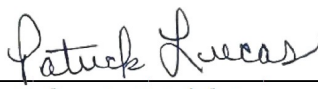
Cordially,



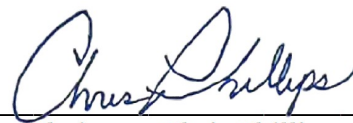
Delegate Tristan Leavitt



Delegate Ryan Browning



Delegate Patrick Lucas



Chairman Chris Phillips

cc: Chairman Robbie Morrie, West Virginia Senate Committee on Government Organization
Speaker Roger Hanshaw, West Virginia House of Delegates
President Randy Smith, West Virginia Senate

¹⁸ <https://www.cve.org/CVERecord/SearchResults?query=flock>; <https://app.opencve.io/cve/?vendor=flocksafety>.

¹⁹ <https://www.flocksafety.com/blog/flock-authorized-as-a-cve-numbering-authority-by-cisa>.