FUSION.LAW

October 29, 2026

by Electronic Mail

Ginger Barry Boyd
NELSON MULLINGS RILEY & SCARBOROUGH LLP
215 South Monroe Street, Suite 400
Tallahassee, Florida 32301

Re: Flock Group Inc. Cease-and-Desist Demand

Ms. Boyd,

I write on behalf of Joshua Michael [redacted] in response to your letter on behalf of Flock Group dated September 25, 2026.

Mr. Michael is an independent cybersecurity researcher who found serious security failures in Flock's systems as part of a good-faith investigation to promote the security of mass surveillance devices. In accordance with accepted cybersecurity research and vulnerability disclosure practice, Mr. Michael reported each vulnerability to Flock first and gave Flock a reasonable opportunity to fix these critical flaws. Flock's response to each was, to put it mildly, underwhelming. More on that below.

Flock, eventually, did remediate the reported vulnerabilities. Only then did Mr. Michael publish a detailed report of his findings along with a formal analysis of the grave threat Flock's vulnerabilities pose to national security and law enforcement operational security.

Flock's response to Mr. Michael's good-faith research and publication has been to defame him to Flock's customers as a "malicious actor," issue spurious trademark notices to his web hosts, falsely accuse him of unlawful conduct, and demand that he remove public-interest materials regarding data Flock allowed to remain publicly accessible.

Mr. Michael's answer to Flock's demand is the reply Brigadier General Anthony McAuliffe gave to German surrender demands at Bastogne during the Battle of the Bulge:

> NUTS!

An elaboration is set out below.

Mr. Michael's Good-Faith Cybersecurity Investigation

As Flock knows, Mr. Michael identified four critical vulnerabilities in Flock's systems. Flock knows this because Mr. Michael reported each vulnerability to Flock first in

accordance with accepted practice for coordinated vulnerability disclosure. Mr. Michael published several papers documenting these four critical vulnerabilities, including a 160-page fully sourced formal report describing his findings in exhaustive detail. Mr. Michael explains throughout these reports the ethical boundaries he observed in refraining from accessing vast amounts of potentially sensitive data that Flock failed to secure: he did not use the access Flock left open to pull police locations, query people or vehicle records, or alter any data.

Flock has presumably studied these findings carefully. Nevertheless, for the record and posterity, we summarize them here:

1. **Hard-coded ArcGIS API key (reported June 11, 2025).** A Flock development environment available on the public internet exposed internal source code containing a live key to Flock's production ArcGIS mapping account. On July 1, 2025, Flock wrote: "We believe this is resolved. Please notify us if you find further issues."
2. **Development application bundles served before login (reported November 13, 2025).** Flock's dev-app.flocksafety.com served its Search and Hotlist application code to anyone, before identification or authentication.
3. **Map credentials issued to anyone who asked (reported November 13, 2025).** Flock's Planner and "Beefeater" sites issued live ArcGIS and Google Maps credentials for Flock's production mapping account to any anonymous visitor. No password, login, or account was required.
4. **FlockNova application bundles served before login (reported December 5, 2025).** Flock's Nova platform served its full client-side application before authentication.

Flock's responses to these reports reveal a concerning habit of ignoring serious vulnerabilities. Mr. Michael did what Flock asked in July 2025: he notified Flock when he found further issues. He sent the November reports on November 13, followed up on November 14, and followed up again on November 19. Flock replied once, on November 19, that it was "internally triaging" the reports and would "reach back out with next steps soon." Flock did not reach back out, with next steps or otherwise, and never responded at all to the December 5 report.

Flock's responses to Mr. Michael's reports, while unsatisfactory in several important ways, demonstrate Flock's understanding that Mr. Michael's research consisted of, and was intended as, good-faith security research undertaken solely for purposes of good-faith

testing, investigation, and/or correction of a security flaw. Flock invited him into its bug bounty program—which he declined, as Flock imposed nondisclosure obligations as a condition of participation, after which Flock confirmed in writing that he was free to publish—and asked him to keep reporting what he found.

The Information Flock Disclosed

Your letter concerns the third critical vulnerability Mr. Michael discovered, which he reported to Flock on November 13, 2025. That same day, Flock published a blog post touting the purported benefits of "people . . . sharing their video footage or license plate reader data with local law enforcement," acknowledging that this kind of powerful surveillance must be "done responsibly, with privacy and transparency at the forefront."

Your letter's description of this vulnerability as "an exposed access key" understates the severity of the security failure. This was not a key someone found on the doorstep then used to enter the house; it was an unlocked screen door that opened for anyone who turned the knob. Analogies are imperfect: Flock's servers issued fresh credentials, on request, to anyone on the internet who asked, without a login of any kind. A system that hands out credentials to anonymous visitors is not a gate.

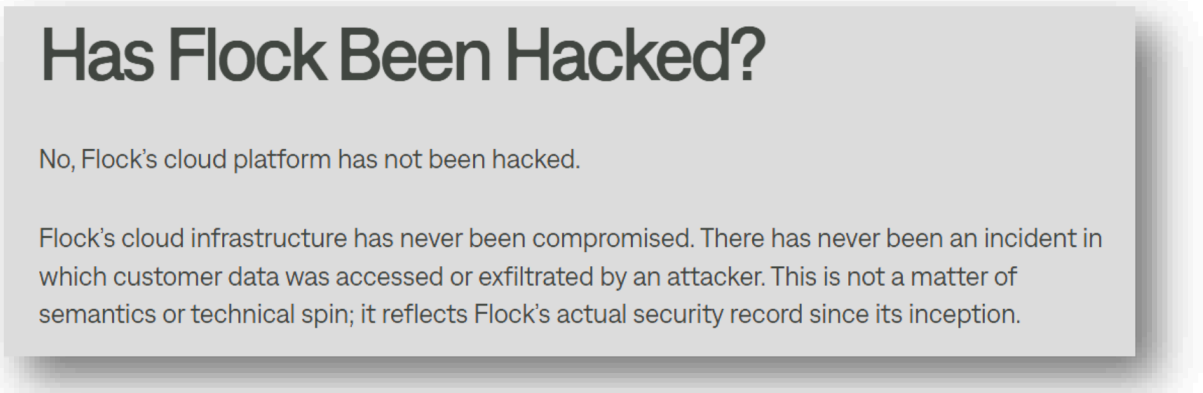
Despite two follow-ups and Mr. Michael's report of yet another—a fourth—critical vulnerability, Flock had not remediated this third vulnerability one month later. On December 14, 2025, the same open path still returned the same credentials to an unauthenticated request. Seeing that Flock had left the information where it was, Mr. Michael took a snapshot of the location data Flock left unsecured.

The Public Interest

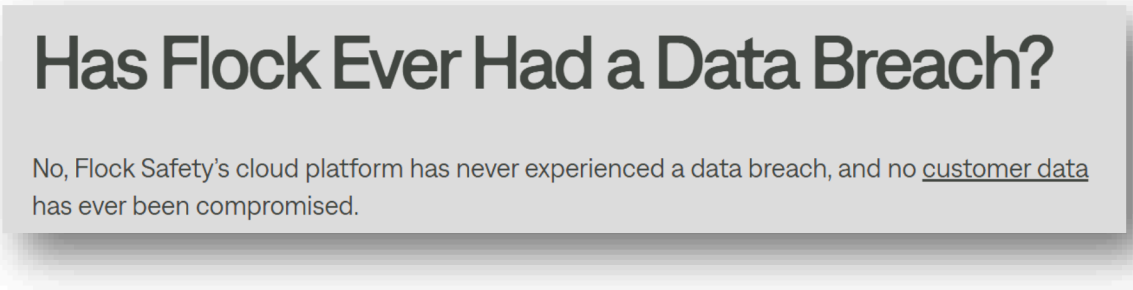
Flock now tells its customers that it "eliminated the vulnerability, and closed the issue in December 2025." Indeed, Flock has spent this year telling the public and its law enforcement customers that its systems have *never* been compromised.

On January 6, 2026, three weeks after the export your letter now calls unlawful, Flock published a page titled "Has Flock Been Hacked?" stating that "Flock's cloud platform has

not been hacked" and that "[t]here has never been an incident in which customer data was accessed or exfiltrated by an attacker."

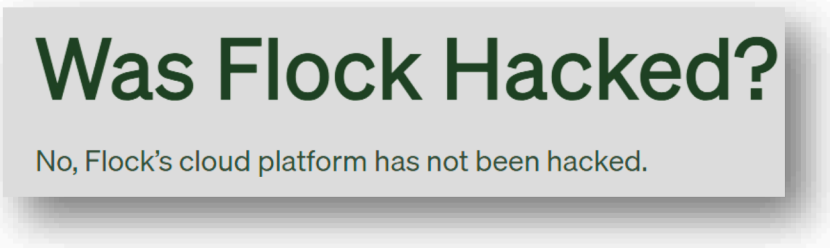


Flock also stated on January 6 that its "cloud platform has never experienced a data breach, and no customer data has ever been compromised":



Those statements have since disappeared from Flock's website. The URL where Flock originally posted them now redirects to a post from September 22. Flock also seems to have excluded its site from the Internet Archive's Wayback Machine. Fortunately, for the public at least, we have an independently archived version of that January 6 post.

Flock's Chief Information Security Officer repeated that position on March 27, 2026, calling contrary claims "false and/or misleading." And Flock said it again on June 10, 2026:



Flock cannot have it both ways. Either Flock knew about the December 2025 export and told the public its data had never been accessed, or Flock did not detect a bulk export of 335,701 records from its mapping interface and told the public its security leads the industry.

Both possibilities highlight the public interest in Flock's security. Mr. Michael's analysis poses important questions on a matter of public concern with serious implications for national security and law enforcement operational security. For example, Mr. Michael's route modeling shows that almost every servicemember at Eglin Air Force Base and Joint Expeditionary Base Little Creek passes a Flock surveillance device going to or from base. Likewise, in the 20-mile FBI Headquarters model, no route was confirmed camera-free.

The purported "substantial costs" that Flock is incurring stem from Flock's cybersecurity shortcomings and its public statements about them, not from the discovery and disclosure of those failings. Mr. Michael carefully avoided any harmful access or disclosure, ethical boundaries unlikely to be honored by an enemy agent or black-hat hacker. If someone used these vulnerabilities to cause Flock harm, it was not my client.

Flock's Demands

With respect to Flock's enumerated demands:

Flock Demand #1: Cease and desist from accessing, attempting to access, or interacting in any manner with any Flock systems, accounts, environments, applications, credentials, services, vendors, or data

Mr. Michael is literally incapable of complying with this request. Like every other American, Mr. Michael does not have the ability to avoid "interacting . . . with any Flock systems," "environments," or "data." Flock surveillance devices are ubiquitous in nearly every major American city. Mr. Michael cannot opt out of interacting with Flock surveillance.

Indeed, Mr. Michael *tried* to opt out of Flock's data surveillance network four times. On October 3, 2025, he asked Flock to stop tracking his license plate; Flock responded that it could not act on individual requests. On November 3, 2025, he asked Flock to delete his personal information; Flock refused. On November 7, 2025, he asked Flock to stop selling or sharing his information; Flock refused the same day. From November 7 through 11, 2025, he asked Flock support how to opt out of the "People Data" processed through FlockNova and Lucidus; Flock referred him to its privacy policy.

In addition, your demand is impossibly vague. For example, Mr. Michael also does not know, and does not intend to try to figure out, who Flock's "vendors" are.

To the extent this demand refers to Flock's electronic web-based data systems, Mr. Michael has not accessed those systems since publishing his good-faith cybersecurity research and does not intend to do so.

Flock Demand #2: Remove any websites, repositories, databases, files, posts, publications, or other materials under your control that make available or disclose information obtained from Flock's systems

Flock Demand #3: Immediately cease any further distribution, disclosure, publication, transfer, sale, sharing, or use of information obtained from Flock's systems

We address these two demands together. The only information Mr. Michael has made available is a matter of public record, including a snapshot of the location of Flock devices as of December 14, 2025.

Flock's systems provided this information to Mr. Michael; it was certainly not "protected." Flock's own servers issued the credential to anyone who asked and, as explained above, Flock left that path open for at least a month after Mr. Michael reported it. Your letter states that "an inadvertently exposed credential is not an invitation to access private systems or data." But this credential was not inadvertently exposed. Flock issued credentials on demand to unauthenticated users and continued to do so for at least a month after it knew this was happening.

There is nothing proprietary or confidential about the *location* of surveillance devices that are visible from public thoroughfares, which is in fact a matter of acute public interest. With respect to law enforcement and other governmental cameras, the location of these surveillance devices is information that *belongs* to the public. As Flock has said again and again and again and again, "Flock customers own their data."

We do not, in any event, take Flock to be asserting that it has a right to surveil American citizens in secret or that its public customers have contracted for such a right. Please do let us know if we are mistaken on this point.

Flock Demand #4: Preserve all documents, communications, logs, records, storage media, accounts, devices, and evidence relating to your access to Flock systems and your acquisition, retention, use, and publication of Flock information

As I told you in my email, we acknowledge your request to preserve potentially relevant records and note that Flock likewise has preservation obligations. I trust that Flock will continue to preserve all relevant documents, communications, and other data, including webpages Flock silently edits or scrubs from its site.

Flock Demand #5: Identify all persons and entities to whom you have disclosed, transmitted, provided, sold, shared, or made available any information obtained from Flock's systems, and identify all locations where that information is stored, maintained, transmitted, or otherwise accessible

Mr. Michael has not sold any information obtained from Flock's systems. The information he has made available is his published good-faith cybersecurity research and supporting data, available at flocksurveillance.org. In addition to his contributions to the public discussion surrounding mass surveillance and national security, Mr. Michael shared his findings and this data with the office of United States Senator Josh Hawley at the request of Senator Hawley's staff.

Flock Demand #6: Provide written confirmation by no later than 5:00 p.m. Eastern Time on September 28, 2026 that you have complied with these demands.

Your letter is dated Friday, September 25, 2026, and demanded a response by the following Monday. That was not a reasonable amount of time. We have responded within a reasonable time.

Reservation of Rights, Etc.

We have tried to make a thorough response to your letter while addressing these and other issues of pressing public concern, and we hope we have resolved any misunderstanding about the nature of Mr. Michael's investigation. We have not, however, undertaken to respond to every assertion; to the extent a point is not addressed here, that omission is not anything like a concession and we trust you will not take it that way. If you have any remaining questions, we encourage you to ask.

Mr. Michael of course reserves all rights, including, among many others, the right to pursue legal recourse for Flock's publication of statements referring to him as "malicious" and other similarly unkind remarks.

Finally, if we have misunderstood your letter or if you believe we have misstated any issue of fact, we welcome further discussion.

Sincerely,



Lee Whitesell
FUSION LAW PLLC
[redacted]
slw@fusion.law

and

David Awad
AWAD LAW P.C.
[redacted]
david@awad.esq