

United States Senate

WASHINGTON, DC 20510

April 24, 2026

JP Guilbault
Chief Executive Officer
Navigate360
3900 Kinross Lakes Parkway, Suite 200
Richfield, OH 44286

Béla Szigethy & Stewart Kohl
Co-Chief Executive Officers
The Riverside Company
45 Rockefeller Center
630 Fifth Avenue
New York, NY 10111

Dear Mr. Guilbault, Mr. Szigethy, and Mr. Kohl:

We write to express significant concern about the risks to students, staff, and schools from a recent cyberattack on your company's P3 Global Intel tip line. We are particularly concerned by reports that the cyberattack exploited platform vulnerabilities in order to steal students' highly sensitive personally identifiable information. We urge you to provide the public clarity regarding what data was stolen, how Navigate360 is responding, and what safeguards Navigate360 will put into place to prevent this from happening again.

According to recent reports, malicious actors breached Navigate360's P3 Global Intel platform last month, stole significant amounts of data, and have since released that data online.¹ More than 35,000 schools and 5,000 public safety agencies use Navigate360's products, meaning that sensitive personal data for millions of Americans may have been stolen.² Schools across the country use Navigate360's P3 Global Intel platform to allow for the safe and secure reporting of safety concerns and threats of violence to school communities. Students also use this resource to report abuse and thoughts of self-harm.

Your company markets its product as an anonymous tip line. However, the personally identifiable information recently released by the hackers suggests otherwise. This puts the safety of students at risk and undermines public trust in using such platforms to report suspicious activity. Education and school safety experts have expressed concerns that, without guaranteed anonymity, students will choose not to report safety concerns.³

¹ Reuters, "Hacker says they compromised millions of confidential police tips held by US company." March 19, 2026. <https://www.reuters.com/legal/government/hacker-says-they-compromised-millions-confidential-police-tips-held-by-us-2026-03-18/>

² Navigate360 landing page, <http://navigate360.com/>. Accessed March 23, 2026.

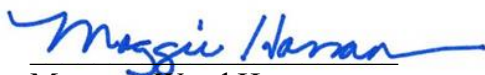
³ Education Week, "A Potential Breach of an Anonymous Tip App Could Have Exposed Sensitive Student Data." March 20, 2026. <https://www-edweek-org.ezproxy.baylor.edu/technology/a-potential-breach-of-an-anonymous-tip-app-could-have-exposed-sensitive-student-data/2026/03#:~:text=Navigate360%20said%20in%20a%20statement,with%20how%20hacktivists%20usually%20work.>

So far, your company has hired an independent third party to investigate the recent cyberattack. We urge you to be transparent with the public about the findings of this investigation, and we request your prompt and comprehensive answers to the following questions:

1. What cybersecurity protections does your company have in place to prevent malicious actors from gaining access? How was the hacker able to circumvent these protections to infiltrate your system?
2. What personally identifiable information was stolen in the data breach? Please clarify whether relevant data related to students, staff, or schools.
3. How many individuals across the United States had their data compromised by the cyberattack? Please provide a breakdown of the number of impacted individuals and schools by state.
4. Are tips submitted through the P3 Global Intel platform fully anonymous, or is personally identifiable information transmitted with the tip or stored in your systems?
5. How many Navigate360 employees have access to any personally identifiable information stored in your systems? What safeguards does Navigate360 have to ensure that personally identifiable information is not shared by employees without authorization?
6. Has Navigate360 ever shared personally identifiable information that it collected through P3 Global Intel with law enforcement, or due to a court order?
7. What assistance have you provided to states, school districts, and schools that were impacted by the data breach, and what supports will you provide them moving forward?

Thank you for your attention to this important matter. We ask that you reply no later than May 8, 2026.

Sincerely,



Margaret Wood Hassan
United States Senator



Jim Banks
United States Senator