

FAQ: Navigate360 Multistate Data Breach

This document provides information regarding the multistate data security incident involving Navigate360, the third-party software vendor for SafeVoice Nevada's anonymous tip platform.

1. What is SafeVoice Nevada?

Established by Nevada Legislature in 2017 through **Senate Bill 212**, SafeVoice provides Nevada students, families, educators, and community members with a 24/7 anonymous platform to report school safety concerns and threats to student well-being. Tipsters submit information via three channels:

- Live telephone call center agents
- The SafeVoice mobile app (forms and chat)
- The SafeVoice online web portal

2. What is Navigate360's relationship with SafeVoice?

The Nevada Department of Education (NDE) and the Nevada Department of Public Safety (DPS) work in partnership to manage SafeVoice Nevada. Navigate360 is a third-party software vendor that contracted with the Nevada Department of Education to provide the digital intake form and backend management system for anonymous tips submitted to SafeVoice. Navigate360 manages only one component of a larger, multi-agency safety infrastructure involving the Nevada Department of Education (NDE) and the Nevada Department of Public Safety (DPS).

3. How widespread was this incident nationally?

While national public reporting varies, estimated media reports indicate that **8.3 million tip records** across Navigate360 data systems were compromised from November 2025 to March 2026. Public reports indicate the incident may have impacted more than 35,000 schools and 5,000 public safety agencies across most states and Canada.

4. What Nevada data was compromised?

In Nevada, state law prevents providing information that could compromise the anonymity of individuals submitting tips. We are able to communicate that a forensic analysis conducted by HaystackID (commissioned by Navigate360) confirmed that the breach occurred between November 2025 and March 2026 and involved **approximately 10% of SafeVoice tips that included personally identifiable information (PII)**.

5. Why were individuals affected not notified directly?

Because SafeVoice is designed as an anonymous reporting line, strict state confidentiality laws

governing SafeVoice prohibit unmasking or attempting to identify anonymous reporting sources. As direct individual notice is legally restricted and technically impossible without unmasking anonymous users, Navigate360 is required by court order to issue a broader **Substitute Public Notice** by the end of October 2026 (likely to be sent Friday, Oct. 23, 2026).

6. What is personally identifiable information (PII)?

A forensic analysis conducted by HaystackID (commissioned by Navigate360) included a broad examination of affected tips that contain personally identifiable information (PII) protected under both Nevada law and the federal Family Educational Rights and Privacy Act (FERPA).

Additional details about the types of PII are below.

Nevada Defines Personally Identifiable Information (PII) in state law:

Under Nevada law (**NRS 603A.040**), PII is defined as an individual's first name or first initial and last name in combination with specific high-risk data elements or unique identifiers, including date of birth, Social Security number, driver license number, and combinations of account credentials and passwords, including financial accounts.

Other Sensitive Tip Data & Unlinked Identifiers that could qualify as PII under the federal Family Educational Rights and Privacy Act (FERPA).

In addition to PII defined by NRS 603A.040, PII related to education is defined by NRS 388.281 and the federal Family Education Rights and Privacy Act (FERPA).

As a result, exposed PII under these definitions include, but is not limited to: student identification number, student name, and name of the student's parent or other family members. It also may include other information such as age, race, medical condition or treatment information, that, alone or in combination, is linked or linkable to a specific student and may reasonably identify a student.

7. What is the timeline of NDE's response?

This timeline is not unique to Nevada, as other states affected by this Navigate360 breach received similar information on or around the following timeline:

Initial Notification

March 2026

Nevada Department of Education (NDE) received initial notification from the CEO of Navigate360 stating that a system breach affecting multiple states had occurred that might involve Nevada's SafeVoice digital intake service. Navigate360 initiated an independent forensic investigation led by HaystackID, while assuring state officials that the active tip submission system remained accessible and operational.

Congressional Inquiry

April 2026

U.S. Senators Maggie Hassan (NH) and Jim Banks (IN) launched a formal Congressional inquiry to demand answers from Navigate360 regarding the multi-state incident.

Preliminary Report Received

June 2026

Navigate360 submitted a preliminary, confidential, and unverified report to NDE suggesting a data breach had occurred, but the scale and scope could not be fully confirmed until a later date.

Navigate 360 Submits Draft Public Notice and Incomplete Data Impact Report to Nevada Department of Education (NDE)/Department of Public Safety (DPS)

September 2026

Upon review of the report submitted, state officials determined the information provided was not sufficient to identify the scope and scale of the breach and lacked actionable detail necessary for public communication. This prompted state officials to demand further verification, investigation, and additional analysis.

Navigate360 submits another incomplete data report

October 6, 2026

After demands made by NDE, Navigate360 delivered another incomplete data impact report. NDE requested further clarification and an analysis of the scale and scope of breached tips that contained PII.

Navigate360 provides additional information about affected data

October 9-15, 2026

Supplemental data regarding scale and scope of PII was delivered on October 9. NDE requested further clarification, which was provided on October 14 and 15.

8. Has the alleged perpetrator been brought to justice?

There is an ongoing investigation by the U.S. Department of Justice.

9. What steps is NDE taking moving forward?

- **Transitioning to a New System:** NDE, supported by the Governor's Office and the Governor's Technology Office, has issued a Request for Information (RFI) to evaluate qualified vendors and transition SafeVoice to a platform with stronger data protections.
- **Ongoing Platform Security:** In the meantime, Navigate360 has confirmed that current daily operations of the SafeVoice 24/7 reporting line remain secure and operational for students and school communities while state authorities work on long-term procurement

solutions.

- **Supporting local leaders:** NDE and DPS will be supporting communication with local school districts and law enforcement to help answer any questions from our school communities. We are also providing guidance issued by Navigate360 for how the public can take steps to monitor and protect their data.
- **Coordinating with state education leaders across the country:** NDE is working with a national organization of state departments of education to explore collective action, report information, and share best practices for ensuring education data vendors protect student data.

10. What steps can I take if my data may have been compromised?

NDE will be sharing guidance from Navigate360 for anyone who may have compromised data. Data and credit monitoring should be utilized for anyone who feels their personal information may have been compromised in this breach, including anyone under the age of 18. Please refer to the guidance document for steps you can take to protect your data.

Navigate360 has created a call center to address specific questions and concerns. Please call 833-966-1754 (toll free) from 6 a.m.-6 p.m. Pacific Time Monday through Friday (excluding U.S. national holidays).