August 25, 2026

The Honorable Andrew Ferguson, Chairman
Federal Trade Commission
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: HISA Data Breach

Dear Chairman Ferguson:

We are writing on behalf of the National Horsemen's Benevolent & Protective Association ("NHBPA"), the North America Association of Racetrack Veterinarians ("NAARV"), and the United States Trotting Association ("USTA"), to bring to the attention of the Federal Trade Commission ("FTC" or "Commission") a serious issue involving the Horseracing Integrity and Safety Act ("HISA") and the security and oversight of the data systems operated by the Horseracing Integrity and Safety Authority ("HISA Authority").

In June 2026, confidential veterinary health information from the HISA Portal appeared on social media, prompting an investigation into how the data had been accessed. HISA initially denied that the information could have come from its portal. Following a roughly two-month investigation that included digital forensics, contractor interviews, and a third-party cyber investigation, HISA ultimately charged Dr. Marshall Gramm, the son of former Sen. Phil Gramm of Texas, on August 17 with improper access to veterinary records and fraud on the betting market.

We want to be clear at the outset: this letter is not intended to excuse or defend Dr. Gramm's conduct. If Dr. Gramm knowingly accessed confidential information concerning horses with which he had no legitimate connection, and used that information for handicapping, wagering, or claiming purposes, then those allegations deserve to be investigated and adjudicated on their merits.

But there is another side to this matter that deserves equal scrutiny: how could an individual using his own log-in credentials repeatedly obtain a huge data set of confidential veterinary information that was outside the scope of his legitimate access, automate the process, and allegedly continue doing so for approximately six weeks without the HISA system detecting and stopping the activity? According to Dr. Gramm, he did not attempt to conceal his identity from the HISA Portal. If that account is accurate, the central issue is not the conduct of an individual user. The more important question is whether HISA had appropriate technical and administrative controls in place to ensure that users could access only the information they were authorized to access.

As you know, HISA is not operating a small private database. It has made a centralized technology platform and centralized data collection a fundamental component of its national regulatory system. HISA's own 2023 Annual Metrics Report described the HISA Portal as containing a broad spectrum of equine treatment and health records and reported that nearly two million veterinary treatment

records had been uploaded to the Portal, with thousands of treatment reports being received daily.[1] That makes the security of this industry information extraordinarily important.

These concerns are heightened considering the substantial resources HISA has devoted to its technology infrastructure. HISA's technology expenditures increased from approximately $6.1 million in 2023 to $10.7 million in 2025. Given this level of investment, it is reasonable to expect HISA to have robust controls in place to prevent and detect unauthorized access to confidential veterinary information. The fact that an individual using his own authorized credentials was apparently able to access sensitive information concerning horses with which he had no legitimate connection raises serious questions about the adequacy of those controls

HISA rightly expects the racing industry to learn from failures and address systemic problems before they happen again. When a horse gets injured, the sport does not simply move on. There is a review of the racing surface, veterinary records, training history, and other available information to determine what happened and whether a systemic problem contributed to the incident. That rigor is intended to identify the underlying cause and prevent the next incident. The same principle should apply here, and HISA should be held to the same standard.

We respectfully urge the Commission to examine this incident and HISA's broader data-security practices with rigor. The confidential health information HISA collects belongs to the horses and industry participants whose information it maintains. Those individuals should be able to expect that the organization entrusted with their information has appropriate safeguards in place to protect it. Specifically, the Commission should consider asking:

- What access controls were originally designed to prevent an authorized user from accessing information outside the scope of that user's legitimate permissions?
- If such controls existed, why did they apparently fail to prevent or promptly identify the activity?
- What monitoring and detection systems were in place?
- Why did automated, repeated requests for information allegedly continue for approximately six weeks without being detected until the information appeared on social media?
- What information was accessed, how much information was obtained, and whose information was affected?
- Who else might have accessed confidential information and not put it on social media for detection?
- What did HISA's internal security personnel identify as the vulnerability?
- What did the independent forensic investigation determine?
- What changes has HISA made to its architecture and access controls since the incident?
- And, perhaps most importantly, who within HISA is accountable for ensuring that the security controls associated with this nationally significant database are adequate?

[1] HISA Releases 2023 Annual Metrics Report (Apr. 3, 2024), *https://hisaus.org/news/hisa-releases-2023-annual-metrics-report*

Additionally, we respectfully ask the Commission, as part of its oversight responsibilities, to condition any future approval of the HISA Authority's budget on the completion of an independent cybersecurity audit, as well as an independent audit of HISA's financial statements. An entity that is spending over $10 million annually on technology should never allow such a basic breakdown of data security to occur. The FTC must demand that the Authority do better, and an audit would help provide the information necessary to implement meaningful change.

The NHBPA is a nonprofit organization representing more than 30,000 owners and trainers of Thoroughbred racehorses throughout the United States. The NAARV is a national organization representing hundreds of equine veterinarians who specialize in the treatment, health, and welfare of racehorses and who understand firsthand the critical importance of maintaining the confidentiality and security of veterinary medical records. The USTA is a not-for-profit organization representing more than 19,500 Standardbred members throughout the United States, who stand to be pulled under HISA's regulatory authority should the HISA Authority survive ongoing constitutional challenges. All three organizations are deeply committed to promoting the care, health, and safety of racehorses, as well as supporting the horsemen and women who participate in the respective sports. We therefore believe strongly that the HISA Authority, the organization entrusted with regulating the horse racing industry, must hold itself to the highest standards of accountability, transparency, and responsibility.

We appreciate the Commission's attention to this matter and would welcome the opportunity to provide any additional information that would assist the Commission in its review.

Respectfully,

Eric J. Hamelback,
CEO, NHBPA

Dr. Andy Roberts
President, NAARV

Douglas K. Daniels, DVM
President and Chairman of the Board

Mike Tanner
CEO, U.S. Trotting Association

Russell Williams
President of the USTA Board

cc: The Honorable Mark Meador, Commissioner