September 9, 2026

The Honorable Andrew N. Ferguson, Chairman
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

The Honorable Mark R. Meador, Commissioner
Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580

Dear Chairman Ferguson and Commissioner Meador,

As the Chief Executive Officer of the Horseracing Integrity and Safety Authority (HISA), I submit this letter to correct and clarify a number of inaccurate and misleading statements contained in the August 28 letter that Churchill Downs Incorporated (CDI), through its Chief Executive Officer Bill Carstanjen, submitted to the Federal Trade Commission (the "Commission").

Mr. Carstanjen opens his letter by asserting that the industry is "still awaiting meaningful answers" regarding the wagering activity associated with the "Fair Hill Five." To the extent he suggests that HISA bears responsibility for providing answers regarding wagering activity, that assertion conveniently overlooks the fact that HISA's congressional mandate does not include the regulation of betting markets and HISA, therefore, has zero authority over wagering activity. HISA will continue to publicly disclose any additional findings related to the conduct of the "Fair Hill Five" that fall within its jurisdiction under the Racetrack Safety Program or Anti-Doping and Medication Control (ADMC) Program, as information becomes available, consistent with its longstanding commitment to transparency.

The apparent criticism of HISA on this topic is particularly interesting given CDI's own position within the industry. In his letter, Mr. Carstanjen describes CDI's ownership of "an advance deposit wagering platform" and the company's "direct and substantial interest" in wagering. It follows, then, that CDI would be uniquely positioned and should be motivated to identify suspicious betting patterns and take action to protect its customers and the industry at large. But, when a horse linked to the "Fair Hill Five" was scheduled to race at a CDI-owned racetrack the very next day, CDI took no action to prevent the horse from racing despite having been made aware of the issue and

presented with an opportunity to act.[1] It was HISA that took the appropriate steps to protect the horse and other racing participants.[2]

CDI's criticism also extends to the timing of the disclosure of an alleged Banned Substance violation. Once again, this appears to be an effort to generate misplaced concern rather than to engage with the relevant facts. In this particular case, the timing of the alleged violation followed the very process that has been in place for approximately the last two years. Public notification of an alleged violation is not made until the B sample is waived or the result is returned confirming the A Sample. If the B sample is waived, public disclosure is made when the notice of violation is served to the Covered Person. If it is not waived, the public disclosure is made following the return of the B Sample. The Horseracing Integrity & Welfare Unit followed HISA's public disclosure procedures to the letter and there was no deviation whatsoever from its standard protocol.

Moving on from the "Fair Hill Five," Mr. Carstanjen transitions to the recent incident involving Dr. Marshall Gramm, a user with access to the HISA Portal, who, with the aid of artificial intelligence, exceeded the scope of his authorized access to obtain horse health information for horses for which he had no legitimate connection. First, I want to be clear that HISA has taken responsibility for and has addressed the system vulnerability that allowed this access to occur and we will continue to work with the Commission, as we always have, to ensure proper oversight over our IT Systems.

Unfortunately, data breaches have become an all-too-common occurrence for organizations maintaining large amounts of data. This includes CDI's account wagering site, TwinSpires.com, who, according to the Paulick Report, was "the victim of a cyber attack" that involved "the intrusion into computer records" in 2012.[3] Additionally, several major companies and organizations with budgets far larger than HISA's have

---

[1] Although CDI has previously excluded trainers from their racetrack where their participation "compromise[s] the integrity of our sport" or "threatens public confidence," CDI took no such action in this case. *See* Horse Network, "Breaking: Churchill Downs Suspends Bob Baffert For Two Years" (June 2, 2021), available at https://horsenetwork.com/2021/06/breaking-churchill-downs-suspends-bob-baffert-for-two-years/. This is not the first time that CDI has refused to act. While Thoroughbred racing in Louisiana continues without HISA oversight due to an injunction awaiting further adjudication, CDI has happily harbored racing participants serving suspensions at HISA racetracks at their New Orleans-based Fair Grounds Race Course. Industry participants serving suspensions under HISA rules, either for Banned Substance violations or for abuse of the crop, have sought sanctuary at Fair Grounds and been happily embraced by CDI management with stalls and entries. *See, e.g.,* The Blood-Horse, "Suspended by HISA, Lopez Continues Riding in Louisiana" (Nov. 13, 2025), available at https://www.bloodhorse.com/horse-racing/articles/288603/suspended-by-hisa-lopez-continues-riding-in-louisiana.

[2] Additionally, HISA promptly moved to provisionally suspend the trainer after additional horses in his care tested positive for Banned Substances, also pursuant to longstanding policy. *See* HISA v. Angel Quiroz, Case No. 2026-19754, available at: https://portal.hisausapps.org/public-ruling/R001744786.

[3] See Paulick Report, "'Small subset of customers affected by security breach at Twinspires.com" (Sept. 4, 2012), available at https://paulickreport.com/news/people/small-subset-of-customers-affected-by-security-breach-at-twinspires-com.

reportedly suffered major data thefts and cybersecurity incidents in 2026.[4] In HISA's case, within weeks of discovering the issue, HISA triggered its cyber insurance policy and retained an independent third-party cybersecurity expert to conduct a forensic investigation, identified Dr. Gramm as the individual responsible, publicly disclosed Dr. Gramm and the vulnerability that was exploited, notified law enforcement, initiated an internal enforcement action against Dr. Gramm and updated our systems to address the exploited vulnerability. In addition, HISA has accelerated the timeline for the independent IT audit required under the Commission's Oversight Rule and is in the process of engaging a third-party auditor to conduct a comprehensive review of its systems, including the vulnerability at issue. The results of that audit will be provided to the Commission, and we look forward to working with the Commission to keep our stakeholders informed on these issues and further strengthen our systems.

HISA has embraced an unprecedented degree of transparency and communication regarding the Gramm incident, engaging directly with stakeholders through press conferences, podcast interviews, public statements and responses to numerous media inquiries.[5] Rather than withholding information pending the conclusion of lengthy investigations, HISA has recognized the importance of earning and maintaining the trust of industry stakeholders and has consistently sought to provide timely, accurate updates and candid explanations regarding the incident.

HISA welcomes and stands ready to answer any and all questions the Commission may have regarding the issues raised in Mr. Carstanjen's letter. We remain confident in the Commission's ongoing oversight and review of our actions, policies, protocols and systems and welcome further conversations on this matter should they be warranted.

Respectfully submitted,

Lisa Lazarus
Chief Executive Officer

---

[4] This includes the McKesson cyberattack impacting millions of records [*see* Inc., "McKesson Supplies 1 in 3 Hospital Prescriptions. Now It's Responding to a Cyberattack Linked to 284 Million Records" (Sept. 1, 2026), available at https://www.inc.com/amaya-nichole/mckesson-supplies-1-in-3-hospital-prescriptions-now-responding-to-cyberattack-284-million-records/91399263], the intrusion and unauthorized access to customer data of home security organization ADT [*see* ADT, "ADT detects cybersecurity incident" (Apr. 24, 2026), available at https://newsroom.adt.com/corporate-news/adt-detects-cybersecurity-incident] and the DentaQuest breach involving the personal and health information of millions of customers [*see* Healthcare Dive, "DentaQuest breach exposes data of 15M people, a record this year" (Aug. 11, 2026), available at https://www.healthcaredive.com/news/Dental-benefits-administrator-discloses-breach/827533/].

[5] A summary of the August 17, 2026 press conference is available on HISA's website: https://hisaus.org/event-recaps/hisa-holds-press-conference-discussing-marshall-gramm-charges.

cc: April Tabor, Secretary, FTC
Lucas Croslow, General Counsel, FTC
Sarah Botha, Special Counsel for HISA, Office of the General Counsel
Charles Scheeler, Chair, HISA
Steve Beshear, Director, HISA
Adolpho Birch, Director, HISA
Leonard Coleman, Director, HISA
Joseph De Francis, Director, HISA
Terri Mazur, Director, HISA
Susan Stover, Director, HISA
Bill Thomason, Director, HISA
DG Van Clief, Director, HISA
William Carstanjen, CEO, Churchill Downs, Incorporated
The Honorable Ted Cruz, U.S. Senate, Texas
The Honorable Maria Cantwell, U.S. Senate, Washington
The Honorable James Comer, U.S. House of Representatives, Kentucky
The Honorable Robert Garcia, U.S. House of Representatives, California
The Honorable Andy Barr, U.S. House of Representatives, Kentucky
The Honorable Paul Tonko, U.S. House of Representatives, New York
The Honorable Brett Guthrie, U.S. House of Representatives, Kentucky
The Honorable Frank Pallone, U.S. House of Representatives, New Jersey
The Honorable Morgan McGarvey, U.S. House of Representatives, Kentucky
The Honorable Mitch McConnell, U.S. Senate, Kentucky