Stay Current

PAUL HASTINGS

March 2026

Follow us on LinkedIn

Litigation Update

Federal Litigation and Enforcement Trends for Colleges and Universities Part 3: The Federal Trade Commission's Expanding Reach Over Nonprofit Institutions

By Ronak Desai, Daniel Prince, David Coogan and Nicole Lueddeke

Colleges and universities have historically operated with the understanding that, as nonprofit institutions, they fall largely outside the jurisdiction of the Federal Trade Commission (FTC). That assumption is increasingly subject to challenge. The FTC has signaled a willingness to scrutinize nonprofit entities whose activities it views as commercial in nature, particularly in areas involving data security, marketing practices, online services, and revenue-generating operations.

For higher education institutions — especially those with complex operational structures, affiliated entities, healthcare systems, research enterprises, and online program management arrangements — FTC risk is no longer theoretical. The agency's evolving jurisdictional posture, combined with its aggressive enforcement agenda in privacy and data security, warrants close institutional attention.

This alert is the third installment in our series examining federal litigation and enforcement risks facing higher education institutions. While Parts One and Two addressed core federal enforcement exposure and downstream litigation risks, this Part Three focuses specifically on the Federal Trade Commission's evolving jurisdictional posture and its implications for nonprofit colleges and universities.

I. Jurisdictional Theories and the "Commercial Activity" Question

The FTC's jurisdiction under Section 5 of the FTC Act generally excludes entities that qualify as bona fide nonprofits. However, the exemption is not absolute. The agency and courts have long recognized that entities organized as nonprofits may nevertheless fall within FTC jurisdiction if:

- They are not truly operating for charitable purposes;
- Their net proceeds benefit for-profit members or affiliates; or
- Their challenged conduct arises from commercial activities closely resembling those of for-profit enterprises.

Modern universities frequently operate through complex structures that blur traditional nonprofit boundaries. These may include:

- Revenue-generating online education programs;
- Executive education and professional certification programs;
- Technology commercialization and intellectual property licensing;
- Research partnerships with private industry;
- Affiliated healthcare systems; and
- Public-private partnerships related to housing, athletics, or campus services.

In assessing jurisdiction, the FTC may examine not only formal corporate status but also functional realities — including governance structures, revenue flows, and the extent to which activities compete in commercial markets.

For institutions with affiliated entities — including foundations, research institutes, or managed service organizations — the jurisdictional inquiry can become fact-intensive. The key risk is not merely whether the university is nonprofit, but whether specific activities could be characterized as commercial conduct affecting consumers.

II. A Test Case for FTC Authority Over Nonprofits

A recent high-profile enforcement action illustrates how the FTC has tested the outer boundaries of its jurisdiction over nonprofit institutions. In late 2023, the Federal Trade Commission filed suit against a large private university and its affiliated service provider, a publicly traded education company, alleging misleading advertising related to advanced degree program costs and representations concerning the university's nonprofit status.

Although the university is organized as a tax-exempt nonprofit, the FTC asserted that its operational structure and financial arrangements — including revenue flows to the publicly traded affiliate — warranted scrutiny under Section 5 of the FTC Act. The complaint alleged that prospective students were misled regarding the total cost of certain advanced programs and that the university's nonprofit representations were deceptive in light of its financial model.

The federal district court dismissed the claims against the university on jurisdictional grounds, concluding that the FTC lacked authority over a bona fide nonprofit corporation. Subsequent administrative and judicial developments reaffirmed the institution's nonprofit status. In August 2025, the Commission voted unanimously to dismiss the action in its entirety.

The FTC's attempt was newsworthy and impactful not because it resulted in a conviction or penalty, but because it publicly tested an expanded interpretation of jurisdiction over nonprofit institutions. The case signaled that tax status alone may not foreclose scrutiny where regulators perceive commercial realities, structural complexity, or consumer-facing representations that resemble those of for-profit enterprises.

III. Data Security and Privacy Enforcement

Data security represents the most immediate and significant area of FTC exposure for higher education institutions. The FTC has made clear that it views unreasonable data security practices as an "unfair" practice under Section 5, even in the absence of a specific sectoral privacy statute.

Universities maintain vast repositories of sensitive data, including:

- Student education records;

- Financial aid and payment information;
- Health and counseling records;
- Biometric and research data;
- Employee information; and
- Alumni and donor records.

Large research institutions also operate sophisticated IT infrastructures that may support federally funded projects, healthcare systems, and international collaborations. Cybersecurity incidents can therefore implicate not only contractual and regulatory obligations, but also consumer protection principles.

The FTC's data security enforcement framework focuses on whether an entity has implemented "reasonable" safeguards in light of the sensitivity and volume of information collected. Enforcement actions in other sectors demonstrate scrutiny of:

- Multi-factor authentication and access controls;
- Vendor oversight and third-party risk management;
- Encryption and data minimization practices;
- Incident detection and response protocols; and
- Board and executive-level cybersecurity oversight.

For universities, a data breach affecting applicants, students, or research participants could prompt parallel exposure: state attorney general investigations, class action litigation, federal agency review (including the Department of Education or HHS, where applicable), Department of Justice False Claims Act investigations, and potential FTC scrutiny if the agency asserts jurisdiction.

Institutions should therefore align cybersecurity governance with enterprise risk management structures and ensure that privacy representations in admissions materials, websites, and vendor contracts accurately reflect operational realities.

IV. Marketing Practices, Online Programs, and Consumer Protection Risk

The FTC has also intensified oversight of marketing and advertising practices in education-related markets. Although much of the agency's recent enforcement has focused on for-profit institutions, the underlying legal theories — deceptive advertising, unfair practices, and substantiation requirements — are not limited by tax status.

Areas of potential scrutiny for nonprofit universities include:

- Representations about job placement rates, graduate earnings, or licensure outcomes;
- Marketing claims associated with online degree programs;
- Statements regarding transferability of credits;
- Tuition pricing transparency; and

- Disclosures concerning financial aid or institutional partnerships.

Universities that contract with online program managers (OPMs), marketing firms, or enrollment consultants should recognize that outsourcing does not eliminate institutional accountability. The FTC routinely applies principles of vicarious liability and expects entities to oversee third-party marketing practices.

As institutions expand digital recruitment strategies — including targeted advertising, influencer partnerships, and data-driven enrollment tools — compliance programs must ensure that public-facing statements are accurate, substantiated, and consistently presented across platforms. Additionally, the marketing and digital initiatives should consider state consumer privacy law requirements. As more states adopt consumer privacy laws, including those that apply to non-profit universities, the FTC may coordinate with state regulators for investigation and enforcement actions related to these initiatives.

V. Institutional Governance in a Multi-Regulator Environment

Importantly, FTC scrutiny does not operate in isolation. The same underlying conduct may draw attention from multiple regulators, reinforcing a central theme across this series: federal enforcement increasingly focuses on institutional governance, internal controls, and documented oversight rather than isolated misconduct.

For example, misrepresentations regarding program outcomes may invite scrutiny from both the FTC and the Department of Education. Cybersecurity failures affecting federally funded research may implicate grant conditions, national security guidance, and consumer protection principles. Inadequate oversight of affiliated entities may raise governance concerns across multiple regulatory frameworks.

Given this convergence, universities should take proactive steps to mitigate exposure:

- **Assess jurisdictional risk.** Evaluate institutional structures, affiliated entities, and revenue-generating activities to determine whether specific operations could be characterized as commercial conduct.
- **Centralize marketing review.** Implement formal review protocols for public-facing representations regarding program outcomes, pricing, and career prospects.
- **Elevate cybersecurity governance.** Ensure board-level or senior leadership oversight of data security, supported by documented risk assessments and briefings.
- **Strengthen vendor oversight.** Enhance contractual safeguards and monitoring for OPMs, marketing vendors, and technology providers.
- **Integrate incident response.** Coordinate breach and regulatory response planning across legal, compliance, IT, and communications functions to address potential multi-agency investigations.
- **Consider insurance coverage**. Understand available insurance policy retentions and limits for cybersecurity incidents and incorporate in incident response.
- **Document diligence.** Maintain contemporaneous records demonstrating risk assessments, corrective measures, and governance oversight.

An important takeaway here is that nonprofit status does not provide categorical insulation from FTC scrutiny. As universities diversify revenue streams and modernize operations, regulators will continue to evaluate whether certain activities resemble commercial conduct affecting consumers. Institutions that align governance, documentation, and public representations with operational realities will be better

positioned to manage the FTC's expanding reach and the parallel proceedings that often accompany federal enforcement.

As the third and final installment in this series, this alert underscores a broader theme across federal enforcement trends: regulators are increasingly focused on institutional structure, governance, and functional realities rather than formal labels. For nonprofit universities, evolving FTC jurisdiction represents a continuation of that shift.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Ronak D. Desai
+1-202-551-1826
ronakdesai@paulhastings.com

Daniel Prince
+1-213-683-6169
danielprince@paulhastings.com

Nicole Dania Lueddeke
+1-213-683-6116
nicolelueddeke@paulhastings.com

David Coogan
+1-212-680-4892
davidcoogan@paulhastings.com