LAW360

Portfolio Media. Inc. | 230 Park Avenue, 7th Floor | New York, NY 10169 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Navigating Enforcement Risks Facing Data Centers

By **Grant Nichols, Yelena Kotlarsky and Alex Blumberg** (July 8, 2025, 4:43 PM EDT)


Grant Nichols


Yelena Kotlarsky


Alex Blumberg

Data centers are an integral part of life and business in the modern economy, and their importance seems to escalate daily alongside advancements in artificial intelligence and other technologies.

Because of their critical function, data center development has exploded across the globe. In the U.S., for example, data centers contribute more than $700 billion to the economy and account for roughly 4.7 million jobs, according to 2023 numbers in a PwC report.[1] And this rise is showing no signs of stopping.

Indeed, along with the hundreds of data centers already under construction, the projected compound annual growth rate of the data center market in the U.S. surpasses 10% per year from 2025 to 2030, according to a data center market summary from Grand View Research Inc.[2] This proliferation, as with many ventures that experience explosive growth, raises a number of potential enforcement risks that data centers may face during development and operation. These risks merit attention whether you are engaged with data centers as an investor, owner or operator.

This article will provide an overview of some of the more pressing enforcement risks to data centers.

Risks During Development and Operation of Data Centers

The legal issues that arise during the development phase relate primarily to the various requirements associated with data center construction. Along with requirements common to all forms of commercial development (e.g., zoning and land use restrictions), data centers typically require special permitting due to their significant consumption of power and water, as well as their overall environmental impact.

Data centers often also need to satisfy additional local protocols such as fire and safety regulations, for example. Understanding these specialized requirements is often complicated because they can vary significantly from local jurisdiction to local jurisdiction.

From an enforcement perspective, the main risks to data centers during development and operation include antibribery and anti-corruption laws, export controls statutes and regulations, and data handling

considerations. Fraud statutes — specifically the False Claims Act, or FCA — are another prominent risk to which we give special focus in the next section.

Antibribery and Anti-Corruption Risks

The high value of data center projects and the surge in investment behind the data center frenzy have the potential to create incentives for cutting corners, misrepresenting capabilities and costs, or taking swift action to secure agreements from power providers or local permitting authorities, all of which create bribery and corruption risk.

Depending on the circumstances — which might also involve activity taken on a company's behalf by third-party contractors or consultants — such actions could put companies at risk of violating antibribery and anti-corruption laws.

These risks are particularly prescient in the data center context, where countries, states and cities are actively competing with each other and engaging in recruitment campaigns — complete with tax breaks and other subsidies — to convince data centers to break ground in their jurisdictions.

With these risks in mind, companies involved with data centers should ensure that they have strong internal controls and monitoring over individuals (both employees and contractors) dealing with local entities on the company's behalf, as well as processes in place to ensure the accuracy and completeness of representations made to government entities.

Export Controls

Relatedly, export control laws pose a potential enforcement risk for data centers and the companies supplying data centers with the components and materials that are critical to their infrastructure.

U.S. export control laws are found in numerous statutes and regulations, and govern the transfer of certain goods — often technological goods — to foreign countries and persons for national security, foreign policy, or other economic reasons. Violations of these various limitations are brought by the U.S. Department of Commerce's Bureau of Industry and Security.[3]

For U.S. companies supplying hardware to data centers that are outside the U.S., export control issues may emerge depending on who ultimately uses those exported materials.

Perhaps the most prominent example at the moment is AI chips, which are high-performance semiconductors and a critical part of data center infrastructure. These AI chips are highly regulated, controlled by the U.S. government and have strong restrictions when exported. For example, it is currently illegal to directly or indirectly export these chips to China.

Additionally, in May, the Bureau of Industry and Security issued guidance to U.S. industry, warning of risks posed by data centers operating as infrastructure-as-a-service training AI models for entities headquartered in China.[4] The Trump administration has signaled that companies should expect strong enforcement of these export controls, which tie into their stated enforcement priority for national security and protecting U.S. intellectual property.

The complex rules regarding end users of advanced technology, especially with increased scrutiny being placed in infrastructure-as-a-service data centers, pose an increased risk that data center stakeholders

need to understand.

Data Handling Considerations

Another category of risk relates to protecting the data center's data — or the information contained in such data — from unauthorized access.

First, data centers that handle certain types of sensitive data need to protect such data from being accessed by countries of concern. The U.S. Department of Justice's newly implemented data security program, which went into effect in April, prohibits or restricts U.S. persons from knowingly directing or engaging in defined classes of transactions that allow persons in countries of concern access to specific categories of sensitive data (e.g., U.S. sensitive personal data and U.S. government-related data).[5]

The referenced countries of concern are China, Cuba, Iran, North Korea, Russia and Venezuela.

Second, data centers that house data from persons or businesses outside the U.S. need to be cognizant of the laws of other jurisdictions as well. Even if the data center is located in the U.S., the extraterritorial reach of many foreign data privacy laws — such as the European Union's General Data Protection Regulation — means that the requirements may still need to be followed by data centers that are physically located elsewhere.[6] One main requirement of these laws is that the data center ensure adequate safeguards for data transfers.

Third, issues with cybersecurity could put data centers at risk of an enforcement action from the government. While there may be a low chance of direct liability on the part of a data center operator for the conduct of individuals using the servers located on its premises, if illegal conduct is being facilitated on-premises, there is a chance that the data center operator might have to deal with the time and reputational risks associated with law enforcement action.

For example, if a data center location has bare metal hosting services that are used to facilitate criminal conduct, then law enforcement might issue subpoenas for information about the operators of that service, their methods of payment, and lease agreements to the data center.

Law enforcement may even issue a search warrant authorizing it to seize a copy of servers from the data center, which may raise difficult issues for the data center operator about notifying the hosting service or data security obligations in its contracts with other collocated hosts at the data center. If foreign cybercriminals or spies are using servers located at a data center, there may also be informal requests for cooperation by U.S. intelligence agencies or formal orders issued under intelligence authorities.

While not a direct threat to the data center operator, such government enforcement and evidence-gathering actions can carry real risks and ask serious questions that a data center operator should consider and plan for in its operational and legal processes.

Representations to the Government: Fraud Risks and the False Claims Act

Criminal and civil fraud statutes — particularly the FCA — pose a significant enforcement risk to data centers and are worth considering in additional detail. Any misrepresentations or exaggerations, which may or may not be intentional, risk creating significant liability for data centers when dealing with government entities.

Significantly, in October 2024, the CEO of a data center company that secured a U.S. Securities and Exchange Commission contract was indicted for deceiving the SEC into thinking that his company's data center was certified at the highest level for reliability and security.[7] In this case, the defendant CEO was charged with six counts of fraud and one count of making false statements to the SEC.

The FCA is a fraud statute that imposes civil liability on any person or company that knowingly presents a false claim to the government for payment.[8] The FCA risk is particularly noteworthy for three primary reasons.

First, FCA liability carries treble damages, which can quickly create significant exposure for companies. Second, FCA cases can be brought in the first instance both by government entities and private relators on behalf of the government. And finally, the Trump administration has stated its intent to enforce the FCA aggressively both generally[9] and when it comes to potential avoidance of tariffs.[10]

In its broadest context, data centers have FCA exposure if they are receiving any form of government funding — even if the funding appears attenuated — and there is some form of ongoing fraud. The risks are widespread in this context because an aggressive enforcement authority or creative relator's counsel could argue that the federal and local government funding or subsidies that many data centers have received create potential FCA exposure.

A sufficient basis for an FCA claim may also arise if the data center is built on public land — which is an initiative actively supported by the current administration.[11]

For example, in July 2024, in Gurion v. Siguler Guff LP, decided in the U.S. District Court for the Southern District of New York, relator Alex Gurion brought a qui tam FCA suit contending that New York private equity firm Siguler Guff fraudulently induced a $150 million loan from the federal agency Overseas Private Investment Corp. (now the U.S. International Development Finance Corp.) by misrepresenting compliance with antibribery and corruption laws.[12]

The complaint also alleged that the firm made various misrepresentations to conceal defaults under the loan agreement. While that case was ultimately dismissed on July 8, 2024, it shows the broad nature of the FCA that can be premised on all sorts of government funding, as well as various types of fraudulent activity.

When it comes to the type of fraudulent activity that may arise uniquely in this industry, a data center should consider the representations that it makes to government entities about its capabilities. The landscape of representations that a data center might make is complex and evolving, but a few examples that could give rise to FCA liability include:

- Representations regarding reliability — that is, certain redundancies to guarantee overall uptime — that a data center certifies to end users, including government entities; and

- Representations about data privacy and security capabilities. For example, data centers may represent an ability to comply with or support complex compliance frameworks such as the National Institute of Standards and Technology or regulatory schemes like the Health Insurance Portability and Accountability Act.

To the extent these capabilities are not accurately or completely described to a government customer or lender, such misrepresentations could give rise to FCA violations.

Along with enforcement of the FCA in its traditional sense, the government could also bring a so-called reverse FCA enforcement action against data centers. This type of action seeks to impose civil liability on any person who knowingly avoids a payment owed to the government. A common type of reverse FCA case is customs fraud. Such cases typically hinge on an allegation that a party made false statements to knowingly and improperly avoid paying money that was owed to the federal government.

Given the significant role that tariffs have played in the Trump administration's trade policy and enforcement priorities to date,[13] reverse FCA cases have the potential to become an important enforcement tool for the DOJ. Tariffs on materials needed for data center construction (e.g., steel and aluminum) and other operating equipment could create risk for companies.

Conclusion

By their nature, enforcement actions typically lag behind an industry's explosive growth as regulators uncover and investigate areas in which potential violations may be occurring. We are just now starting to see the emergence of data center enforcement actions a few years behind the start of the data center boom.

We expect an increase in data center enforcement actions moving forward.

Grant Nichols and Yelena Kotlarsky are partners, and Alex Blumberg is a senior associate, at King & Spalding LLP.

King & Spalding associate Joseph Hendricks contributed to this article.

[1] PWC, Economic Contributions of Data Centers in the United States: 2017-2023 (Feb. 2025), accessible at https://www.centerofyourdigitalworld.org/2025-impact-study.

[2] Grand View Research, Data Center Market Size, Share, & Trends Analysis Report By Component (Hardware, Software), By Type (On-premise), By Server Rack Density, By Redundancy, By PUE, By Design, By Tier Level, By Enterprise Size, By End Use, By Region, And Segment Forecasts, 2025 – 2030, https://www.grandviewresearch.com/industry-analysis/data-center-market-report.

[3] See generally King & Spalding, Client Alert: New Data Center Validated End User Program Creates Pathway to Export Advanced U.S. Technology; Rigorous Review and Vetting Required (Oct. 15, 2024), available at https://www.kslaw.com/news-and-insights/new-data-center-validated-end-user-program-creates-pathway-to-export-advanced-us-technology-rigorous-review-and-vetting-required.

[4] See generally King & Spalding, Client Alert: Department of Commerce Issues Export Controls on Advanced Computing Chips and Artificial Intelligence Models (Jan. 30, 2025), available at https://www.kslaw.com/attachments/000/012/469/original/ca013025.pdf?1738346170.

[5] See Department of Justice: Office of Public Affairs, Justice Department Implements Critical National

Security Program to Protect Americans' Sensitive Data from Foreign Adversaries (Apr. 11, 2025), https://www.justice.gov/opa/pr/justice-department-implements-critical-national-security-program-protect-americans-sensitive.

[6] See European Union, General Data Protection Regulation, https://gdpr-info.eu/.

[7] Office of Public Affairs | Data Center Company CEO Indicted for Major Fraud and Making False Statements to the U.S. Securities and Exchange Commission | United States Department of Justice.

[8] For purposes of clarity, this article simply refers to the FCA to cover potential liability under both the federal FCA as well as state FCA statutes. Most state FCA statutes are modeled after the federal FCA, but there can be important differences. For example, the New York FCA uniquely applies to tax fraud and avoidance – which is barred by the federal FCA.

[9] See Daniel Wilson, DOJ Official Flags 'Aggressive' FCA Approach Under Trump (Feb. 20, 2025), https://www.law360.com/articles/2300751/doj-official-flags-aggressive-fca-approach-under-trump.

[10] Dep't of Justice, Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime (May 12, 2025), accessible at https://www.justice.gov/criminal/media/1400046/dl?inline.

[11] See Ashleigh Fields, Trump Administration Announces Plans to Build AI Data Centers on Federal Land (Apr. 3, 2025), https://thehill.com/homenews/administration/5230334-trump-ai-data-centers/.

[12] See generally King & Spalding, Siguler Guff Wins Dismissal in FCA Suit (July 10, 2024), https://www.kslaw.com/news-and-insights/siguler-guff-wins-dismissal-in-fca-suit.

[13] Dep't of Justice, Focus, Fairness, and Efficiency in the Fight Against White-Collar Crime (May 12, 2025), accessible at https://www.justice.gov/criminal/media/1400046/dl?inline.