Trade Secret Quarterly

July 2026

Data Centers at the Center of Trade Secret Disputes

As data centers multiply across the United States, they are raising novel questions about how companies can protect confidential information that depends on third-party infrastructure. Companies now claim trade secret protection not only for code and customer data, but also for the design, construction, and operational specifications of the facilities that keep that information moving. The harder companies work to keep those operations under wraps, the more curious the public seems to become. Public utilities add another complication because they often must disclose records about data centers' communications with public entities and utility use. The result is a catch-22: companies need data centers to keep pace with technological advancement, but those same facilities can expose highly sensitive information to misappropriation and disclosure risk.

Can a Data Center's Design Be a Trade Secret?

A Florida appellate decision in *Digiport, Inc. v. Foram Development BFC, LLC*, 314 So. 3d 550 (Fla. 3d DCA 2020), illustrates the first issue: whether a data center's design and operation can qualify as a trade secret. Digiport alleged that it confidentially proposed a centralized data/collocation center for the Brickell Financial Centre, where tenants could rent space for computer hardware or use Digiport's cloud computing and management services. After Digiport gathered technical information, the parties discussed how to incorporate the proposed data center into the building. The deal fell through, and Foram hired another company to design and install a data center that offered many of the services Digiport had proposed. Digiport sued, alleging trade secret misappropriation. The Florida appellate court reversed summary judgment on Digiport's FUTSA claim, finding that a factual dispute remained over whether Digiport's proposed project combined otherwise readily ascertainable components in a way that could qualify for trade secret protection. That holding illustrates that in data center disputes, a design need not be patent-style novel if the unified combination gives the owner economic value because others cannot readily ascertain it by proper means.

Public Demand for Transparency Adds Complexity

The second issue flows from the industry's appetite for power and water. Because data centers consume extraordinary amounts of both, they often depend on public utilities that operate under broad public records laws. Two recent high-profile disputes in Wisconsin – one involving a Microsoft-owned facility and another involving a Meta facility – show the tension. In both cases, advocacy groups used public records requests to seek detailed electricity and water usage information, triggering fights over whether public utilities must release that operational data or companies can shield it as competitively sensitive. The disputes expose a structural mismatch: private operators want confidentiality, while the public utilities that serve them often must deliver transparency.

Together, these developments signal that companies relying on data centers, and companies designing and operating them, should reassess the contractual, technical, and regulatory measures used to protect competitively sensitive information. Strong NDAs, tailored disclosure protocols, tight vendor access controls, and early engagement with public utility commissions will likely become standard parts of a defensible trade secret protection program for data center stakeholders.

Trade Secret Litigation Trends: Increased Enforcement, Inconsistent Awards, Rise in State-Law-Only Claims

Trade secret litigation keeps evolving, and plaintiffs do not always get predictable results. Recent data points to three trends: (1) companies are filing more trade secret and intellectual property cases; (2) damages awards remain unpredictable; and (3) plaintiffs are increasingly relying on state-law-only claims. Together, these trends show that trade secret protection matters more than ever and weak protection programs can create expensive litigation risk.

Filing volume tells the first part of the story. Federal trade secret filings have climbed steadily for several years, reaching record highs and reflecting a roughly 30% increase over the past decade. In 2025, federal trade secret case filings surged, with 1,552 new filings, a 20% increase over 2024 and the highest annual total since Congress enacted the Defend Trade Secrets Act (DTSA). AI-related trade secret filings also continued to grow, jumping 92% in the second half of 2025 compared with the first half. Dismissal rates, by contrast, have remained relatively steady, with courts dismissing a consistent fraction of the docket on threshold grounds each year. These numbers show that companies are turning to trade secret litigation more often to protect confidential and proprietary information.

Damages tell a messier story: awards to successful parties span an unusually wide range. Headlines focus on damage awards that are in the range of hundreds of millions of dollars, but most awards are more modest. The takeaway is straightforward: recovery depends heavily on a disciplined damages model that connects the requested award to specific, proven trade secrets. That damages model can be based on several theories. One is actual damages, which compensate for direct losses caused by misappropriation. This is a foundational theory, but difficult to prove when the trade secret misappropriation does not result in a distinct loss of business. A second is an unjust enrichment theory, which focuses on the defendant's gains, rather than the plaintiff's losses. This may be applicable, for instance, when a defendant saves time and money in jump-starting a new product or design by utilizing the trade secret information. Yet another option is to seek a reasonable royalty, which attempts to determine what a willing licensee would have paid a willing licensor for the opportunity to use the trade secret information. Regardless of which theories are used, jurors want plaintiffs to connect the dots clearly between theft and quantifiable damages.

The rise in state-law-only claims shows another strategic shift. Although the DTSA continues to anchor many federal filings, plaintiffs increasingly pair federal claims with state-law claims, and state-law-only filings now represent a meaningful and growing slice of trade secret litigation. The reasons vary by case, but they typically include forum considerations, the scope of remedies available under particular state regimes, and concerns about federal pleading standards.

In the second half of 2026, companies should expect more enforcement activity and build protection programs accordingly. This means identifying and documenting specific trade secrets before a dispute arises, both to support liability theories and to enable the disaggregated damages presentations that recent appellate decisions demand. Companies should also decide at the outset of a dispute whether a state-law-only claim better serves their strategic objectives than a federal DTSA claim. Either way, rising enforcement and unpredictable damages raise the stakes for employers who need airtight confidentiality and intellectual property clauses to prevent employee misuse of trade secrets.

Washington's Noncompete Ban Gets Teeth

Washington has moved the garden variety noncompete off the menu. On March 23, Governor Bob Ferguson signed HB 1155, which takes effect June 30, 2027, and makes all noncompetition covenants "void and unenforceable," regardless of when the parties signed them. That is a material change from the 2019 framework, which preserved noncompetes for certain higher-earning workers and treated post-employment restrictions longer than 18 months as presumptively unenforceable rather than categorically barred.

For employers whose value lives in source code, pricing strategy, customer goodwill, business plans, or employee know-how, the takeaway is not that those assets are suddenly unprotectable, but rather that Washington wants those interests protected with sharper tools – confidentiality agreements, trade secret and invention protections, carefully drafted nonsolicitation covenants, and certain reimbursement or transaction-related covenants – not broad restraints on where someone works next.

Now Banned

- Employment and independent contractor noncompetes that prohibit or restrain a worker from engaging in a lawful profession, trade, or business are void and unenforceable.
- Customer "no-business" restrictions are treated as noncompetes if they directly or indirectly prohibit accepting or transacting business with a customer, patient, or client.
- Forfeiture-for-competition provisions are also swept away: a clause that requires someone to return, repay, or forfeit a right, benefit, or compensation because they engage in lawful work may be deemed a noncompetition covenant.
- Employers may not enforce, threaten to enforce, represent that a worker is subject to, enter into, or attempt to enter into a noncompetition covenant.

Still Available

- Employee nonsolicitation covenants remain available to prohibit a former employee from soliciting current employees to leave the employer.
- Customer, patient, and client nonsolicitation covenants may still prohibit solicitation of current or prospective customers, patients, or clients to shift business away from the former employer, but the statute now ties that protection to relationships the employee established or substantially developed through work and limits the restriction to 18 months after termination.
- Confidentiality agreements and covenants prohibiting the use or disclosure of trade secrets or inventions remain outside the noncompete ban, and HB 1155 does not amend Washington's trade secrets statute.
- Written agreements to repay out-of-pocket educational expenses remain permissible if they expire within 18 months of the employee's start date, are prorated for the remaining portion of that 18-month period, and release the employee from repayment if the separation is for good cause.
- Sale-of-business covenants remain available for a person purchasing or selling business goodwill or otherwise acquiring or disposing of an ownership interest, but only if the signer buys, sells, acquires, or disposes of an ownership interest representing at least 1% of the business.
- Certain franchise-sale covenants entered into by a franchisee also remain outside the definition of a noncompetition covenant when the franchise sale complies with Washington's franchise sale requirements.

Suggested Actions for Employers with Washington Employees

- Inventory employment, independent contractor, equity, bonus, severance, deferred compensation, training repayment, and commission plans for language that restricts competition, blocks acceptance of customer business, or triggers forfeiture because of competitive activity.
- Identify current and former employees and independent contractors whose noncompetes may still be within their effective period, and prepare written notices before the October 1, 2027, deadline.
- Replace "you cannot work for or do business with" language with more narrow confidentiality, trade secret, invention, or nonsolicitation provisions that fit the statutory carveouts.
- Tighten trade secret hygiene: update access controls, exit certifications, device return procedures, download monitoring, and manager training so the company can protect valuable information without leaning on a banned noncompete.
- Train HR, recruiting, sales, and managers not to tell workers they are bound by a noncompete after the effective date, because that representation itself can violate the statute.

Takeaways

The back-end risk is real. Beginning June 30, 2027, violations can lead to the greater of actual damages or a $5,000 statutory penalty, plus reasonable attorneys' fees, expenses, and costs. By October 1, 2027, employers also must make reasonable efforts to notify current and former employees and independent contractors whose noncompetes are still within their effective period that those covenants are void and unenforceable.

In short: Washington did not ban employers from protecting clients, confidential information, or trade secrets – it banned garden variety noncompetes. The employers best positioned for 2027 will be those who replace broad post-employment restraints with precise, provable protections for the relationships and information that actually need protection.

FOR MORE INFORMATION

For more information, please contact:

Deborah S. Brenneman
513.352.6638
Deborah.Brenneman@ThompsonHine.com

Brittany A. Mallow
216.566.5654
Brittany.Mallow@ThompsonHine.com