Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Trade Secrets 2026

Definitive global law guides offering
comparative analysis from top-ranked lawyers

USA – D.C. Metropolitan Area: Trends and Developments

Linda M. Jackson, Andrew Baskin, Pascal "Pat" Naples
and John M. Hindley
ArentFox Schiff LLP

USA – D.C. METROPOLITAN AREA

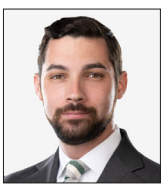
Trends and Developments

Contributed by:
Linda M. Jackson, Andrew Baskin, Pascal "Pat" Naples and John M. Hindley
ArentFox Schiff LLP

ArentFox Schiff LLP is internationally recognised in core industries where business and the law intersect. Its trade secrets practice comprises 35 partners and 24 other lawyers firm-wide, combining IP, employment, white-collar, and transactional capabilities. Known for rapid-response injunction work, complex multi-forum disputes, cross-border discovery, and strategic counselling, we advise clients across industries and jurisdictions. Significant 2025 trials include representing as plaintiff in Fairfax County, Virginia a leading government contractor against a competitor and a former employee, including complex data spoliation claims, and representing as defendant in the federal district court in Baton Rouge, Louisiana a major pipe manufacturer in a cross-border licensing dispute. Other current matters include representing as plaintiff a global petrochemical company in the Delaware federal district court and representing as defendant in the new Texas Business Court a leading software developer for commercial airlines. Recent counselling work includes trade secret audits and drafting employment policies and non-compete agreements for clients in artificial intelligence, food and beverage, financial services, and pharmaceuticals.

Authors

Linda M. Jackson is a co-leader of ArentFox Schiff's Complex Litigation Practice Group and Trade Secrets, Noncompetes & Employee Mobility Group. Her practice centres on trade secrets misappropriation, restrictive covenants, employment and commercial litigation, whistle-blower matters, and high-stakes internal investigations. She represents clients in federal and state courts nationwide, with expertise in the District of Columbia, Eastern District of Virginia "Rocket Docket", and Virginia state courts. Trusted by boards and senior executives, Linda handles C-suite investigations and advises on executive mobility, non-compete, and confidentiality strategies. She is recognised by Chambers USA for DC General Commercial Litigation and Labor & Employment.



Andrew Baskin is a partner in ArentFox Schiff's Complex Litigation group based in Washington, DC. His practice focuses on trade secrets, restrictive covenants, employment, and labour relations. Andrew was a member of the trial team representing CACI, Inc., prosecuting claims and securing injunctive relief in federal litigation involving competitive procurements valued at more than USD500 million. He has considerable experience advocating on behalf of employers in state and federal court, during collective bargaining, and at arbitration. Andrew also offers counsel before administrative agencies and conducts internal investigations involving discrimination and harassment claims.

Contributed by: Linda M. Jackson, Andrew Baskin, Pascal "Pat" Naples and John M. Hindley, **ArentFox Schiff LLP**

Pascal "Pat" Naples is a senior associate at ArentFox Schiff in Washington, DC. His practice focuses on trade secret and non-compete disputes, government investigations, and litigation, particularly in health care. Pat was a member of the trial team representing CACI, Inc., prosecuting claims and securing injunctive relief in federal litigation involving competitive procurements valued at more than USD500 million. He is a primary author of the firm's Annual Trade Secrets End of Year Report. He clerked at the US Court of Federal Claims and the US Court of Appeals for the Fourth Circuit's Office of Staff Counsel.

John M. Hindley is an associate at ArentFox Schiff in Washington, DC, focusing on commercial litigation and government investigations, including trade secret and non-compete matters. He is one of the primary authors of the firm's Annual Trade Secrets End of Year Report and biweekly Trade Secrets Case Watch blog. John was a member of the trial team representing CACI, Inc., prosecuting claims and securing injunctive relief in federal litigation involving competitive procurements valued at more than USD500 million. Prior to joining ArentFox Schiff, John clerked for the Honorable William E. Smith, US District Court for the District of Rhode Island.

ArentFox Schiff

1717 K Street NW
Washington, DC
20006 USA

Tel: 1 202 775 5785
Fax: 1 202 857 6395
Email: linda.jackson@afslaw.com
Web: www.afslaw.com

Trade secret law continues to evolve rapidly, including within the Washington, DC–Maryland–Virginia region (DMV). As businesses confront new competitive pressures, emerging technologies, and a shifting legal landscape around restrictive covenants, understanding and navigating trade secret protections has never been greater. This feature surveys the DMV's key legal frameworks; examines national trends shaping trade secret litigation, including under the federal Defend Trade Secrets Act (DTSA); and offers practical strategies for protecting trade secrets as non-compete agreements face growing restrictions.

Trade Secret Protection in Washington, DC, Maryland, and Virginia

Each state within the DMV has enacted its own version of the Uniform Trade Secrets Act with several similarities. Fundamentally, each jurisdiction defines "trade secret" in essentially the same way: information that (i) derives independent economic value from not being generally known to, or readily ascertainable by, others who could benefit from its disclosure, and (ii) is the subject of reasonable efforts to maintain its secrecy. Moreover, each jurisdiction prohibits misappropriation by "improper means", defined to include theft, bribery, misrepresentation, breach or inducement of a breach of a duty to maintain secrecy, or espionage through electronic or other means. Each trade secrets statute has a three-year statute of limitations.

Courts can enjoin actual or threatened misappropriation. Additionally, in each jurisdiction, a plaintiff can recover both actual loss and unjust enrichment caused by misappropriation or, alternatively, a reasonable royalty. And if the misappropriation was wilful and malicious, a court may award exemplary damages and attorneys' fees.

The DMV's statutory frameworks offer relative consistency and predictability in protecting confidential and proprietary information.

Washington, DC: The District of Columbia Uniform Trade Secrets Act (DCUTSA)

DCUTSA, D.C. Code § 36-401 et seq., provides the statutory framework for trade secret protection in the District. The threshold inquiry in every trade secret case is whether there is a trade secret to be misappropriated. "[I]nformation is not a trade secret as a matter of law if it is easily ascertainable by the public or generally known within an industry". *Econ. Rsch. Servs. Inc. v Resol. Econs., LLC*, 208 F. Supp. 3d 219, 232–33 (D.D.C. 2016). To determine if something is a trade secret, DC courts have relied on the six-factor test articulated by the Restatement of Torts § 757. Courts have recognised that customer lists, pricing information, business plans, and other compilations of business information can constitute trade secrets under the statute. Importantly, a combination of public information can constitute a trade secret if the combination adds value to that information.

To achieve trade secret status, the plaintiff must demonstrate reasonable efforts to maintain secrecy, not absolute secrecy. In *Meyer Group, Ltd. v Rayborn*, for example, the court held that alleging that employees were required to sign confidentiality agreements was enough at this stage to plausibly allege the existence of trade secrets under both DTSA and DCUTSA. No 19-1945, 2020 WL 5763631, at *6 (D.D.C. Sept. 28, 2020). Other measures courts have credited include maintaining information on password-protected computer systems with restricted access, implementing employee policies on the importance of maintaining confidentiality, marking documents as confidential, keeping physical copies in locked file cabinets, and including confidentiality notices in email communications.

DCUTSA defines "misappropriation" to encompass two categories of wrongful conduct: (i) acquiring a trade secret while knowing or having reason to know it was acquired by "improper means", and (ii) disclosing or using a trade secret without express or implied consent where the person used improper means to acquire knowledge of the trade secret, or knew or had reason to know their knowledge of the trade secret was derived from someone who utilised improper means, and acquired it under circumstances giving rise to a duty of secrecy, or obtained it by accident or mistake. Because misappropriation can rarely be proved by direct evidence, plaintiffs often rely on circumstantial evidence. For example, in *Aristotle International, Inc. v Acuant, Inc.*, the court found that, under both DTSA and DCUTSA, the plaintiff stated a trade secrets claim based on circumstantial evidence

where the defendant announced an acquisition shortly after requesting the plaintiff's confidential information and declined to certify its destruction or return. No 22-cv-741, 2023 WL 1469038, at *9 (D.D.C. Feb. 2, 2023).

Standing to bring a misappropriation claim is a significant issue. Though some courts describe DTSA and the DCUTSA as identical, an important textual difference is that the DCUTSA does not limit those who can bring trade secrets claims to "owners"; rather, it permits "complainant[s]" to bring claims for misappropriation. Though DC courts have yet to address this issue, Maryland courts applying similar language in the Maryland trade secrets statute (discussed below) recognise that, unlike DTSA, standing is not limited to owners but rather may include other parties, such as legitimate holders of trade secrets.

Maryland: The Maryland Uniform Trade Secrets Act (MUTSA)

To prevail on a MUTSA claim, the plaintiff must show: "(1) that [the plaintiff] possessed a valid trade secret, (2) that the defendant acquired its trade secret, and (3) that the defendant knew or should have known that the trade secret was acquired by improper means". *AirFacts, Inc. v de Amezaga*, 909 F.3d 84, 95 (4th Cir. 2018); see Md. Code Ann., Com. Law § 11-1201 et seq.

Like DCUTSA, courts applying MUTSA are guided by the Restatement of Torts § 757 to determine if information is a trade secret. Maryland courts have recognised that a wide range of information can qualify as a trade secret, including customer lists, pricing information, profit margins, vendor pricing, marketing strategies, and budget software, so long as the information derives independent economic value from not being generally known and the owner takes reasonable measures to maintain its secrecy. See *Ingram v Cantwell-Cleary Co., Inc.*, 306 A.3d 1205, 1228–34 (Md. App. 2023). For example, the Fourth Circuit reversed a lower court's post-trial finding that information was not a trade secret because it contained publicly available information. AirFacts, 909 F.3d at 96. It reasoned that, although the trade secret contained data that can be accessed by anyone with a subscription, the defendant spent months compiling the data in particular groupings and applying his expertise to display that compiled information in a useful format.

As to reasonable efforts to maintain secrecy, Maryland courts have taken a totality of the circumstances approach. Common measures recognised as reasonable include requiring employees and third parties to sign confidentiality or non-disclosure agreements; maintaining employee handbooks with confidentiality provisions; implementing electronic security measures such as password-protected systems, encrypted servers, and firewalls; limiting access to trade secret information on a need-to-know basis and restricting the number of employees who can view sensitive data; and labelling documents as confidential.

MUTSA incorporates the same definition of "misappropriation" as DCUTSA. Under MUTSA, a plaintiff can prove misappropriation "simply by demonstrating that the defendant acquired the trade secret by improper means, even if the plaintiff cannot show use of that trade secret". *Brightview Grp., LP v Teeters*, 441 F. Supp. 3d 115, 132 (D. Md. 2020). Because direct evidence of misappropriation is often unavailable, plaintiffs may rely on circumstantial evidence as proof.

MUTSA permits "complainants" to bring a claim, meaning that possessors of a trade secret can sue for misappropriation. *AirFacts*, 909 F.3d at 95. Unlike DTSA, ownership is not a prerequisite to bringing a Maryland trade secrets claim.

Virginia: The Virginia Uniform Trade Secrets Act (VUTSA)

In analysing VUTSA, Va. Code § 59.1-336 et seq., Virginia courts have recognised that "just about anything can constitute a trade secret under the right set of facts", including customer lists, pricing information, marketing and sales techniques, and information about products. *MicroStrategy Inc. v Business Objects, S.A.*, 331 F. Supp. 2d 396, 416 (E.D. Va. 2004). This is because the "crucial characteristic of a trade secret is secrecy rather than novelty". *Dionne v Se. Foam Converting & Packaging, Inc.*, 397 S.E.2d 110, 113 (Va. 1990). Such efforts include the use of confidentiality agreements, marking and controlling

access to documents with proprietary information, and using firewalls.

The Supreme Court of Virginia's landmark decision in *Appian Corp. v Pegasystems, Inc.*, 924 S.E.2d 621 (Va. 2026) clarified several aspects of VUTSA. The case involved the reversal of a USD2 billion jury verdict where Pegasystems is alleged to have used a "spy" to access Appian's internal website to gather confidential and proprietary information. The Court held that VUTSA "applies to any information that meets the statutory definition, whether that be computer code, a marketing plan, or even undisclosed and not publicly ascertainable strengths and weaknesses of a product". To that end, the Court interpreted VUTSA's definition of "trade secret" to broadly include "any information that provides actual or potential economic value to those who rightfully possess it and that is not 'readily ascertainable' through legitimate means by others 'who can obtain economic value from... disclosure or use' of the information, so long as the rightful possessor of the information has taken 'reasonable' steps under the circumstances to maintain the secrecy of the information". It further confirmed that secrecy need not be absolute; trade secrets "can be disclosed to a million people and remain protected" so long as the disclosures are "made in confidence, express or implied". It also held that by adopting a reasonableness standard, the state legislature "made clear that VUTSA requires neither bank vault nor armed-guard-style protection to maintain trade secret protection". To obtain damages, the Court emphasised that complainants bear the burden of establishing a "causal connection" between the defendant's wrongful conduct and the claimed damages. Said differently, plaintiffs must show they were harmed and that the wrongful conduct proximately caused the harm.

VUTSA defines "misappropriation" substantially in the same way as DCUTSA and MUTSA. Unlike DCUTSA and MUTSA, the Virginia statute defines "improper means" to include "use of a computer or computer network without authority". Importantly, misappropriation can still occur even where the defendant did not use improper means to acquire the trade secret if the defendant subsequently disclosed or used that secret in violation of a duty or without consent. *Variable Annuity Life Ins. Co. v Coreth*, 535 F. Supp. 3d 488, 513 (E.D. Va. 2021).

Spoliation often arises in trade secrets litigation. Virginia's recently passed statute, Va. Code § 8.01-379.2:1, addresses a party's duty to preserve evidence and how courts should address spoliation. The statute provides that parties have a duty to preserve evidence that, based on the totality of the circumstances, may be relevant to reasonably foreseeable litigation. If such evidence is lost due to a party's failure to take reasonable preservation steps and cannot be restored or replaced through additional discovery, a court may remedy the spoliation in two ways. First, upon finding prejudice to another party, the court may order measures no greater than necessary to cure the prejudice. Second, if the court finds that the spoliating party acted recklessly or intended to deprive another party of evidence, the court may presume that the evidence was unfavourable to the spoliating party, issue an adverse inference instruction, or dismiss the action or enter a default judgment. See *Order, CACI, Inc.–Fed. v Schilling*, No 2021-16925 (Va. Cir. Ct. Apr. 23, 2024) (unpublished) (granting default judgment against ex-employee who engaged in reckless and wilful spoliation, including repeatedly wiping devices subject to a court-ordered forensic examination).

Like the DC and Maryland statutes, VUTSA authorises "complainant[s]" to sue for misappropriation. Consistent with the statute, the Court in Appian Corp. discussed the definition of "trade secret" to broadly include any information that provides economic value "to those who rightfully possess it" and described how a trade secret "holder" must maintain secrecy.

National Trends and Issues Concerning Trade Secrets and DTSA Claims

Precision in defining a trade secret

Courts are increasingly demanding precision in the identification of trade secrets. The Fourth Circuit in *Sysco Machinery Corp. v DCS USA Corp.* held that both DTSA and state trade secret statutes require a plaintiff to identify "with sufficient particularity" the trade secret it claims has been misappropriated. 143 F.4th 222, 228–29 (4th 2025). Failure to do so may lead to dismissal, like in *JTH Tax LLC v Cortorreal*,where the court dismissed a DTSA claim because the plain-

tiff's complaint listed categories of information without describing the material or how it derived economic value from it. No 2:23-cv-0355, 2024 WL 897605, at *6 (E.D. Va. Mar. 1, 2024). At the same time, courts have acknowledged that plaintiffs need not plead the content of the trade secrets themselves. See *Trilogy Fed. LLC v CivitasDX LLC*, No 24-cv-2713, 2025 WL 436850, at *4–5 (D.D.C. Feb. 2, 2025) (finding that descriptions of "detailed multi-step strategies" and "specific steps to be taken" in the context of government-contracting proposals were sufficiently particular).

DTSA's extraterritorial reach

DTSA's extraterritorial reach continues to develop. The statute can apply to foreign conduct only if the defendant is a US citizen or entity organised under US laws, or "an act in furtherance of the offense was committed in the United States". 18 U.S.C. § 1837. In *dmarcian, Inc. v dmarcian Europe BV*, the Fourth Circuit confirmed this framework, finding that retrieving trade secrets from servers located in the United States and facilitating their use or disclosure within the foreign country satisfied the domestic-nexus requirement. 60 F.4th 119, 141–42 (4th Cir. 2023). Courts have since applied this standard to both sustain and dismiss DTSA claims. In *GTY Technology Holdings Inc. v Wonderware, Inc.*, a court found the domestic nexus satisfied where former employees and a foreign defendant met in Chicago to conspire to take trade secret information. No 24 CV 9069, 2025 WL 1455762, at *8 (N.D. Ill. May 21, 2025). By contrast, in *Whaleco Inc. v Shein Technology LLC*, the court dismissed a DTSA claim where all the alleged misappropriation occurred in China and the plaintiff pleaded no facts showing any "act in furtherance" within the United States. No 23-3706, 2025 WL 2801861, at *16–17 (D.D.C. Sept. 30, 2025).

Intensifying trade secrets litigation: more filings and higher verdicts

Trade secret litigation intensified again in 2025, with outsized verdicts and consequential appellate guidance. Juries issued large damages awards, though many were subsequently reduced on appeal or post-trial. In *Appian Corp.*, which involved a jury award exceeding USD2 billion for trade secret misappropriation under VUTSA, the Virginia Supreme Court affirmed the Court of Appeals' reversal and remanded for a new trial, addressing important questions about the proper burden of proof for damages. Other large jury awards include a USD452 million award in *Insulet Corp. v EOFlow (D. Mass)* and USD70 million in *TriZetto v Syntel Sterling (S.D.N.Y)*. Such decisions illustrate both the high stakes and the volatility of trade secrets litigation.

Spoliation

Spoliation remains a recurring and critical issue in trade secret cases. Courts have shown increasing willingness to impose severe sanctions, including default judgment, for intentional, bad-faith spoliation. In *Atlantic Diving Supply, Inc. v Komornik*, the court imposed adverse inference sanctions after finding that the defendants had engaged in a pattern of destroying evidence, including deleting communications and using encrypted messaging platforms to avoid detection. 113 Va. Cir. 179, 187–94 (Va. Cir. 2024). Other courts have entered default judgment (also known as a "termination sanction") for intentional spoliation where ex-employees wiped storage devices and laptops, concealed evidence, deleted data or emails, and violated discovery-related orders. See *BalanceCXI, Inc. v Int'l Consulting & Rsch. Grp., LLC*, No 1:19-CV-0767-RP, 2020 WL 6886258, at *13–14 (W.D. Tex. Nov 24, 2020);*WeRide Corp. v Huang*, No 5:18-CV-07233-EJD, 2020 WL 1967209, at *11–16 (N.D. Cal. Apr. 24, 2020). Plaintiffs should retain forensic experts early, pursue expedited discovery, and document preservation failures to obtain redress for spoliation where appropriate.

Emerging technology and AI issues

Artificial intelligence is transforming components of trade secret jurisprudence. Emerging questions include the extent to which AI training or deployment practices risk waiving trade secret protection if protective measures are not robust and ownership boundaries around compilations generated through joint development. Courts are beginning to address how AI-driven software platforms are identified and protected as trade secrets, with decisions emphasising that a plaintiff must identify the specific technical contours of the trade secret, not merely describe what the software is intended to accomplish.

Protecting Trade Secrets in the Face of Narrower Non-Compete Enforceability

For decades, non-competes served as a crucial tool for protecting trade secrets, but recent federal executive action, legislation, and judicial decisions have altered the legal landscape.

With respect to the federal government, the FTC pursued and then abandoned its attempted nationwide ban on non-competes. That said, the FTC remains engaged in selective enforcement litigation. To that end, the FTC launched a Joint Labor Task Force in February 2025, held a non-compete workshop in January 2026, and has issued warning letters to large healthcare employers advising them to audit their non-competes.

State-level legislation has created an increasingly difficult legal landscape. In 2025 alone, at least 11 states enacted non-compete restrictions. Currently, DC imposes income thresholds, position restrictions, notice requirements, and durational limitations on non-competes; Maryland imposes income thresholds and restrictions specific to healthcare providers and veterinarians; and Virginia imposes income thresholds and, starting 1 July 2026, will broadly ban non-competes, except if termination is for cause or the non-compete provides for severance.

Meanwhile, some courts have grown increasingly unwilling to "blue pencil" overbroad provisions to save them from invalidity.

Given these developments, businesses should consider alternatives to non-competes in safeguarding their trade secrets. Below, we examine several such strategies.

Confidentiality and nondisclosure agreements

Confidentiality and nondisclosure agreements (NDAs) remain broadly enforceable and may be expressly exempted from state-level non-compete restrictions. To maximise their protective value, businesses should define with specificity the categories of confidential information – such as customer lists, pricing strategies, proprietary formulas, and research data – rather than relying on vague, overbroad definitions that courts may deem unenforceable. NDAs should clearly articulate an employee's obligations during and after employment, including the duty to return or destroy confidential materials upon departure, and should establish ongoing confidentiality obligations that survive termination where appropriate. When properly drafted, NDAs provide robust trade secret protection without the enforceability risks increasingly associated with non-competes.

Non-solicitation agreements

Depending on the state, non-solicitation agreements – which restrict a departing employee's ability to solicit the former employer's clients, customers, or employees – may be viewed more favourably than non-competes because they do not prevent an individual from taking another job. To enhance enforceability, businesses should limit restrictions to clients or client prospects with meaningful relationships with the departing employee, or existing clients, prospects, or employees about whom they may have proprietary information – eg, compensation details.

Forfeiture-for-competition provisions

Forfeiture-for-competition provisions condition the receipt of certain benefits, like deferred compensation, equity, or severance, on compliance with non-competition obligations. Because the employee retains the freedom to compete, and simply faces a financial consequence for doing so, courts have been less hostile to these provisions. Businesses using this approach should ensure the provision applies to a meaningful benefit, clearly defines competitive activity, and specifies the time period and consequences of a violation.

Tailoring agreements to jurisdiction-specific requirements

One takeaway from the foregoing discussion is the significant variability across jurisdictions in enforcing restrictive covenants. In some states, non-solicitation provisions may be viewed, either by statute or based on precedent, in the same manner as non-compete provisions. In other states, the same may be true of forfeiture-for-competition provisions. Still other states might treat both of those provisions as distinct from non-competes. Given this variability, employers with employees in multiple states must tailor their employment agreements to the appropriate jurisdiction; a one-size-fits-all approach can be fraught.

Contributed by: Linda M. Jackson, Andrew Baskin, Pascal "Pat" Naples and John M. Hindley, **ArentFox Schiff LLP**

Robust information security and governance

Ultimately, contractual protections are only as strong as the operational measures supporting them. Businesses should formally identify and catalogue trade secrets, assign custodians, and implement secrecy measures proportionate to the sensitivity of the assets. These measures should include access controls, encryption, physical security, electronic security, document classification systems, and clear internal policies governing the handling of confidential and proprietary information. Organisations should regularly audit these practices, as documenting reasonable secrecy measures is critical to prevailing in any subsequent trade secret misappropriation claim.

Monitoring employee departures

Businesses should review access logs for unusual data activity around employee departures, conduct forensic reviews of departing employees' devices and accounts, and enforce data deletion and property return protocols. Clear offboarding procedures create a contemporaneous record that can prove invaluable in subsequent recovery and enforcement actions.

Litigation readiness

Even with strong preventive measures, trade secret misappropriation may occur, and the speed and precision of the legal response can be decisive. Courts increasingly demand that plaintiffs identify their trade secrets with specificity at the outset of litigation. Among other things, this entails establishing relationships with experienced outside counsel and developing protocols for evidence preservation and rapid response to potential misappropriation, as it may be critical to obtain injunctive relief quickly to prevent irreparable harm.

Conclusion

The narrowing scope and enforceability of non-compete agreements do not leave businesses without recourse to protect their trade secrets. A robust, multi-layered trade secret programme and protection strategy can effectively safeguard a company's most valuable proprietary information.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com