JONES DAY

GLOBAL TRADE SECRET UPDATE

KEY DEVELOPMENTS IN 2025

Introduction

This publication summarizes noteworthy 2025 legal developments in trade secret law in key centers of commerce throughout the world. Understanding these legislative and judicial developments can help trade secret owners maintain trade secret protection, guard against misuse of their trade secrets by others, and assert rights as necessary.

Table of Contents

continued on page iv


KEY DEVELOPMENTS IN
THE UNITED STATES

IDENTIFYING PROTECTABLE TRADE SECRETS

Ninth Circuit Finds that the Sufficiency of a Trade Secret Disclosure in Discovery Is a Question of Fact

Quintara Biosciences, Inc. v. Ruifeng Biztech, Inc., 149 F.4th 1081 (9th Cir. 2025)

The Ninth Circuit Court of Appeals recently decided a case of significance regarding a plaintiff's disclosure of its asserted trade secrets under the Defend Trade Secrets Act ("DTSA"). Quintara Biosciences, Inc., a DNA-sequencing-analysis company, brought suit in a California federal district court against Ruifeng Biztech, Inc., alleging misappropriation of trade secrets under the DTSA.[1] At the outset of discovery, Ruifeng moved the court for a protective order to halt discovery until Quintara further specified its trade secrets. Ruifeng made its request consistent with California Code of Civil Procedure Section 2019.210, which requires that a plaintiff identify its trade secrets with reasonable particularity before obtaining discovery into a defendant's technology.

While there was no California Uniform Trade Secrets Act ("CUTSA") claim in the case, the district court cited Section 2019.210 in ordering Quintara to further identify its trade secrets. Ultimately, Quintara did not identify its trade secrets to Ruifeng's satisfaction, and Ruifeng again moved to halt discovery. To end the discovery standoff, the district court gave Ruifeng a choice to either accept the disclosure and comply with discovery or move to strike the disclosure and accept the consequences if wrong. Ruifeng moved to strike the trade secrets in the disclosure under Federal Rule of Civil Procedure 12(f). Drawing on Section 2019.210, the district court granted the motion, striking nine of 11 trade secrets. The district court acknowledged that the state procedure did not govern, yet it applied that "reasonable particularity" rule "to nail down [Quintara's] asserted trade secrets … [and] permit [the court] to discern the reasonable bounds of discovery."[2]

On appeal, the Ninth Circuit reversed the order striking the asserted trade secrets. The court explained that CUTSA's disclosure rule does not govern a DTSA claim and stated that under the DTSA, it is a question of fact whether a trade secret has been sufficiently identified in a disclosure. Thus, "whether a plaintiff has sufficiently particularized a trade secret under DTSA is usually a matter for summary judgment or trial."[3]

The Ninth Circuit held that the circumstances did not warrant the harsh penalty of dismissal of Quintara's claims as a sanction for failure to comply with a pretrial order under Federal Rule of Civil Procedure 37. Among other things, the Ninth Circuit noted that the district court did not consider alternatives before striking Quintara's trade secrets (including that after an opportunity for discovery on the identification of trade secrets, the district court could have invited a motion for summary judgment and, absent a genuine fact dispute as to whether the trade secrets were sufficiently particularized, could have granted summary judgment as to those trade secrets). Accordingly, the Ninth Circuit held that it was error for the district court to strike and functionally dismiss trade secret claims as a discovery sanction as part of the trade secret disclosure process.[4]

Quintara builds on prior Ninth Circuit cases stating that a plaintiff must sufficiently identify its trade secrets in order to prevail on the merits of a trade secret claim. *See InteliClear, LLC v. ETC Glob. Holdings, Inc.*, 978 F.3d 653 (9th Cir. 2020); *Imax Corp. v. Cinema Techs., Inc.*, 152 F.3d 1161 (9th Cir. 1998).

The holding in *Quintara* does not resolve the question of whether a DTSA defendant can insist on a sufficient trade secret identification before providing technical discovery. Nor does *Quintara* speak to the standard for pleading a DTSA claim. *Quintara* makes it clear that, for a defendant to prevail on grounds of insufficient particularity of a trade secret, the defendant usually must wait for summary judgment or trial to show that the trade secrets were not sufficiently identified.

Fourth Circuit Affirms Dismissal for Failure to Meet Sufficient Particularity Requirement

Sysco Mach. Corp. v. DCS USA Corp., 143 F.4th 222 (4th Cir. 2025)

Sysco Machinery Corporation, a manufacturer of rotary die cutting machines, sued its former distributor, DCS USA Corporation ("DCS"), for trade secret misappropriation. Sysco alleged that DCS sold counterfeit machines made by a Sysco competitor. According to Sysco, the competitor produced those machines using information stolen from Sysco. Sysco brought trade secret misappropriation claims against DCS under the DTSA and the North Carolina Trade Secrets Protection Act, in addition to several other claims. The instant lawsuit was Sysco's third attempt to bring a federal lawsuit against DCS, after the first two—which included the competitor and were filed in different districts—were dismissed.

The court emphasized that pleading a trade secret misappropriation claim requires some specificity given that "it is the type of claim that has the potential to seriously disrupt ordinary business relationships."

The district court dismissed Sysco's claim for trade secret misappropriation under Rule 12(b)(6) for failure to state a claim "because it was stated in 'broad, sweeping terms' that, 'absent factual enhancement,' lacked the specificity needed to be cognizable."[5] The district court also denied Sysco's subsequent request to alter or amend the judgment and for leave to amend its complaint, finding that Sysco's behavior across its three civil actions called into question whether it had engaged in bad faith pleading practice.[6]

The Fourth Circuit affirmed the district court's dismissal of Sysco's trade secret misappropriation claims, holding that Sysco failed to plausibly allege either a valid trade secret or misappropriation. Sysco failed to identify its claimed trade secrets with sufficient particularity because its shifting trade secret definitions, in different parts of its complaint and at oral argument, forced the defendant and the court "into a fishing expedition to find evidence of a valid trade secret in the pleadings" from which the court "emerged empty-handed."[7] At various points during litigation, Sysco identified the following as trade secrets:

- "Sysco's compilation of machinery, software, and confidential information,"[8]
- "Sysco's proprietary and confidential information, including the Copyrighted Works, and technical, financial, operations, strategic planning, product, pricing vendor, and customer information,"[9] and
- "'[T]he technical documents, test videos, statistical data, client contracts, and other confidential information used by Sysco to develop and manufacture' rotary die cutting machines."[10]

According to the court, these definitions "suggest that nearly Sysco's entire business is a trade secret" and were so "sweeping and conclusory" that they prevented DCS from knowing what it was accused of misappropriating, and prevented the court from evaluating whether Sysco met the reasonable measures and independent economic value requirements.[11]

Other aspects of the complaint also doomed Sysco's claims. First, the court held that Sysco's claimed trade secrets like the "Copyrighted Works" included public information, which is ineligible for trade secret protection.[12] Second, the court held that Sysco's complaint failed to plausibly allege misappropriation because it "did not make clear how DCS acquired, disclosed, or used its trade secrets."[13] The court emphasized that pleading a trade secret misappropriation claim requires some specificity given that "it is the type of claim that has the potential to seriously disrupt ordinary business relationships."[14]

Fourth Circuit Finds Existence of Confidentiality Provision Sufficient to Demonstrate Reasonable Measures at the Pleading Stage

Samuel Sherbrooke Corp. Ltd v. Mayer, 149 F.4th 252 (4th Cir. 2025)

Samuel Sherbrooke Corp. ("Sherbrooke"), an insurance company, along with its majority shareholder, sued three former employees for trade secret misappropriation under the DTSA for using proprietary software in a competing business. Sherbrooke's employment contract contained the following confidentiality agreement: "[The employee] shall not . . . use or exploit Confidential Information for any purpose other than for the benefit of . . . [Sherbrooke]."[15] The contract further included an "Inventions Provision," which stated that any invention created with any of Sherbrooke's confidential information shall "become the sole and exclusive property of [Sherbrooke]."[16] One of the three employees developed Sherbrooke's proprietary software, which enabled Sherbrooke to more effectively predict risk values and price insurance contracts.

The district court granted the defendants' motion for judgment on the pleadings, finding that Sherbrooke did not plausibly allege that the information was kept secret through commercially reasonable measures simply because the employees were subject to confidentiality agreements.[17] The district court also found allegations that the defendants actively used the proprietary software "to assist with operating this new competing insurance entity" to be "general and conclusory."[18]

Evaluating the district court's grant of judgment *de novo* under the Rule 12(b)(6) standard, the Fourth Circuit reversed the district court on both findings.[19] The Fourth Circuit explained that "what may constitute 'reasonable measures' must be considered in light of the nature of the trade secret and the context in which it exists."[20] Although it acknowledged other cases where plaintiffs alleged more than a signed confidentiality agreement, the Fourth Circuit did not require Sherbrooke to allege more, and found no reason to create such a requirement.[21] It was enough that Sherbrooke required the employees to sign the employment contract, which was sufficiently connected to the proprietary software.[22] Finally, the court found allegations that the defendants created or otherwise knew about the proprietary software, and then "created a competing business and used the [p]roprietary [s]oftware to assist that competing business," sufficient to state a claim for misappropriation.[23]

Third Circuit Elaborates on "Independent Economic Value" Requirement

NRA Grp., LLC v. Durenleau, 154 F.4th 153 (3d Cir. 2025)

A debt collection firm, the National Recovery Agency Group, LLC ("NRA"), sued two former employees for trade secret misappropriation under the DTSA and the Pennsylvania Uniform Trade Secrets Act ("PUTSA"), among other claims, for creating and emailing a spreadsheet containing one of the employees' passwords to access "dozens of NRA systems and accounts" while still employed by NRA.[24] The passwords granted access to NRA's "business records and customer databases,"[25] which contained "consumer PII and other private information."[26] On cross-motions for summary judgment, the district court granted summary judgment to the former employees on all of NRA's claims. Regarding the trade secret claims, the district court held that because the passwords did not have "independent economic value," they were not trade secrets under federal or state law.[27]

The Third Circuit agreed with the district court that the passwords were not trade secrets under the DTSA and PUTSA and affirmed summary judgment on that basis.[28] The Third Circuit referenced case law where password information was bundled with other, more colorable trade secrets, and noted that passwords may have "economic value" in some circumstances.[29] However, the spreadsheet at issue here—merely a compilation of passwords—had no "independent economic value" under both the DTSA and the PUTSA.[30] The court reasoned that the passwords themselves were not the "product of any special formula or algorithm."[31] The Third Circuit also reasoned that NRA "misses the point entirely" by arguing about the sensitivity and economic value of the underlying customer information that the passwords protected.[32] Instead, the passwords were mere "numbers and letters" that protected the information with actual independent economic value: "[I]t is what the passwords protect, not the passwords, that is valuable."[33] Indeed, NRA was able to immediately and easily remedy the theft by simply changing the passwords, underscoring the court's conclusion that they lacked *independent* economic value.

District Court Addresses Protectability of Unreleased Music

PleasrDAO v. Shkreli, No. 24-cv-4126, 2025 WL 2733345 (E.D.N.Y. Sep. 25, 2025)

PleasrDAO, a company that collects and displays culturally significant media, sued a former pharmaceutical executive and now-convicted fraudster, Martin Shkreli, for trade secret misappropriation under the DTSA and New York law, among other claims. The alleged trade secret: the lone copy of the never-before-released Wu-Tang Clan album *Once Upon a Time in Shaolin*. Shkreli bought the album for $2 million in 2017 but was forced to forfeit it when he was convicted of securities fraud. PleasrDAO purchased the album in 2021 for $4 million. In the years that followed, Shkreli admitted to retaining and distributing copies of the album, played portions of the album during live streams on social media platforms, and posted comments online taunting PleasrDAO about his possession of the album. Shkreli moved to dismiss the trade secret claims against him, arguing that PleasrDAO failed to plead that the album is a trade secret.

Although some courts have held that unreleased musical works do not meet this standard because the value of the unreleased recordings is derived from the right to sell the recording to the public, this case was different.

The court disagreed, denied Shkreli's motion, and held that PleasrDAO sufficiently alleged that the album was a trade secret.[34] The court acknowledged that the case presented an unusual application of the trade secret doctrine, and that the album did not fit squarely within a category of business information or data traditionally protectable as a trade secret.[35] A key issue was whether PleasrDAO sufficiently alleged that the album derived independent economic value from not being generally known, particularly given that the album consisted of unreleased musical work subject to restrictions.

Although some courts have held that unreleased musical works do not meet this standard because the value of the unreleased recordings is derived from the right to sell the recording to the public, this case was different. PleasrDAO could not distribute the album widely—it owned the album subject to numerous usage restrictions that, among other things, forbid public commercial release. Its business model was focused on collecting culturally significant media to create unique "ecosystem experiences."[36] PleasrDAO sufficiently pled that the album had independent economic value based on PleasrDAO's ability to exploit its exclusivity to create an "experience" that its competitors could not.[37]

Tenth Circuit Affirms Summary Judgment for Failure to Identify Protectable Trade Secrets

Double Eagle Alloys, Inc. v. Hooper, 134 F.4th 1078 (10th Cir. 2025)

Double Eagle Alloys, Inc. sued its former employee Michael Hooper and his new employer Ace Alloys, LLC for trade secret misappropriation under the DTSA and the Oklahoma Uniform Trade Secrets Act ("OUTSA"). When Hooper left Double Eagle, he took his handwritten notes and 2,660 digital files downloaded from his Double Eagle computer. Double Eagle claimed that the files contained three types of trade secrets: (i) pumpshaftquality ("PSQ") specifications; (ii) Double Eagle's pricing model (including margins and material costs); and (iii) customer drawings. The district court granted summary judgment to the defendants on all claims, holding Double Eagle failed to identify its trade secrets with sufficient particularity and that the information was not sufficiently secret or confidential to qualify.[38] On appeal, the Tenth Circuit affirmed.[39]

As to the PSQ specifications, the Tenth Circuit held Double Eagle failed to identify with particularity what portions of those specifications were not readily ascertainable from public sources.[40] The evidence at summary judgment showed that substantial portions of Double Eagle's PSQ specifications had been made publicly available by Double Eagle and were otherwise known in the industry. And Double Eagle failed to point out to the court what portions of its "thousands of pages" of specifications were not publicly available.[41] Double Eagle "merely point[ed] to the specifications without distinguishing the trade secret information from the rest," and "provided no information on how they qualify as trade secrets."[42]

Double Eagle's pricing model also did not qualify as a trade secret.[43] As the Tenth Circuit explained, the pricing model was not a trade secret because Double Eagle shared its prices with its customers, and did not prevent those customers from further sharing them.[44] Although Double Eagle doubled down on appeal and argued its pricing model could be a trade secret, it failed to point the court to sufficient evidence: Its affidavits and spreadsheets lacked detail demonstrating a unique or proprietary methodology, the effort or resources expended to develop the model, or a distinct competitive advantage derived from its secrecy.

Under the DTSA, the claim failed at the threshold because Double Eagle does not own the drawings. They are created by customers and supplied to distributors for quoting, and the DTSA requires the plaintiff to be the owner of the trade secret.

The court also held that the customer drawings do not qualify as trade secrets under either the DTSA or OUTSA.[45] Under the DTSA, the claim failed at the threshold because Double Eagle does not own the drawings. They are created by customers and supplied to distributors for quoting, and the DTSA requires the plaintiff to be the owner of the trade secret. Under the OUTSA, the drawings are readily ascertainable by proper means—customers routinely share them with distributors and others in the quoting process, and the record lacked evidence of broad, enforceable confidentiality restrictions across customers.[46] The court found that a single confidentiality agreement with one customer was insufficient to show non-ascertainability or secrecy of the category as a whole, particularly where evidence showed third parties could and did obtain the drawings from sources other than Double Eagle.[47] Accordingly, the drawings could not support trade secret claims under either statute.[48]

NEW EMPHASIS AGAINST DOUBLE RECOVERY

Third Circuit Provides Guidance for Trade Secret "Use" and Impermissible Double Recoveries

Harbor Bus. Compliance Corp. v. Firstbase.io, Inc., 152 F.4th 516 (3d Cir. 2025)

Firstbase.io, Inc. and Harbor Business Compliance Corporation formed a partnership to develop a compliance software product for Firstbase. After the parties' relationship deteriorated, Firstbase took control of the product and began offering services without Harbor's input or support. Harbor sued Firstbase and won on its claims for breach of contract, unfair competition, and trade secret misappropriation. Part of the jury's damages award included approximately $11 million for trade secret misappropriation and nearly $15 million for unfair competition. On appeal, the Third Circuit issued two notable holdings under the DTSA and the Pennsylvania Uniform Trade Secrets Act.

First, the court held that there was sufficient evidence of misappropriation by use.[49] Firstbase argued mere similarities between the parties' products were insufficient to prove use because those similarities do not rule out independent development.[50] The court rejected this argument, noting other circumstantial evidence supported the jury's finding that Firstbase used Harbor's trade secrets.[51] To make this point, it pointed to "plus factors" that suggested that Firstbase did not independently develop the technology.[52] These plus factors included: (i) internal Firstbase communications suggesting that it was using Harbor information; and (ii) Firstbase's "accelerated nationwide launch" of its product.[53]

Second, the court held that the jury improperly awarded Harbor duplicative damages.[54] The jury awarded Harbor $14,757,399 in damages for its unfair-competition claim, the same amount of Firstbase's profits calculated by Harbor's damages expert.[55] And the jury's trade secret misappropriation award ($11,068,044) amounted to 75% of the total profits, which was used because the jury found that Firstbase misappropriated 75% of Firstbase's trade secrets.[56] According to the court, "[t]his was double recovery of the same remedy and not a coincidence."[57] The Third Circuit reduced the award by $11,068,044, allowing Harbor to accept the discounted award or elect a new damages trial on its trade secret claims.[58]

District Court Requires Plaintiff to Choose Between Injunction and Full Damages Award

Insulet Corp. v. EOFlow, Co., 779 F. Supp. 3d 124 (D. Mass. 2025)

Insulet Corp. ("Insulet") sued EOFlow, Co. Ltd., EOFlow, Inc., Nephira Bio, EOFlow's CEO, and three former Insulet employees under the DTSA for misappropriating its trade secrets relating to the design and manufacturing of an insulin patch pump, the Omnipod. After a month-long trial, the jury awarded Insulet $452 million in damages ($170 million in unjust enrichment damages and $282 million in exemplary damages) for willful and malicious misappropriation of three of its four asserted trade secrets. Insulet then moved for a permanent worldwide injunction "to prohibit defendants from using, possessing, selling, or otherwise distributing plaintiff's trade secrets," and to preserve the jury's damages award.[59] The defendants asserted the permanent injunction would be impermissible double recovery and that the scope of the injunction was unduly broad.

The district court granted the permanent worldwide injunction.[60] As it explained, a worldwide injunction was appropriate because the defendants had "already attempted to sell the trade secrets" to a foreign competitor. As to the duration of the injunction, the court noted that a permanent injunction, although uncommon, was appropriate under the circumstances because there was no evidence that the trade secrets could be independently developed in a specified amount of time. Indeed, the evidence showed competitors had invested millions trying to develop the product to no avail. As part of the injunction, the court also reassigned patent applications that derived from Insulet's trade secrets and permitted Insulet to audit defendants up to two times a year.

After awarding the injunction, the court noted that it overlapped with the jury's unjust enrichment award, resulting in double recovery.[61] After all, the unjust enrichment damages were "based in substantial part on defendants' future, unrealized gains."[62] So the court gave Insulet a choice: (i) keep the injunction and accept a reduced damages award that accounted only for defendants' then-existing profits; or (ii) keep all the damages but forgo the injunction. The plaintiffs elected reduced damages and an injunction. Thus, the court reduced the damages award to $59.4 million: $25.8 million in unjust enrichment damages (avoided costs) and $33.6 million in exemplary damages.[63]

NEW CHALLENGES TO NON-COMPETES

Federal Developments

FTC Abandons Appeals of Vacatur of 2024 Final Rule that Sought to Establish a Blanket Ban on Non-Competes. On September 5, 2025, the FTC voted 3–1 to dismiss its appeals in the 5th and 11th Circuits, agreeing to the vacatur of the Biden-era Final Rule.[64] But although the FTC has abandoned the Final Rule, non-competes continue to be a subject of agency scrutiny.

Following its withdrawal of the appeals of the 2024 Final Rule, the FTC's focus is on a more targeted enforcement of over-broad non-competes as "unfair methods of competition."

Targeted Section 5 Enforcement Remains an FTC Priority. Following its withdrawal of the appeals of the 2024 Final Rule, the FTC's focus is on a more targeted enforcement of over-broad non-competes as "unfair methods of competition." Specifically, the FTC announced that it will leverage its power under Section 5 of the FTC Act to initiate enforcement actions against entities it has reason to believe are engaged in "unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[65] Based on recent statements by FTC commissioners, the FTC is likely to evaluate agreements based on an employee's skill and wage level, deployment across distribution networks, agreements with independent contractors, the likelihood of freeriding, the availability of less restrictive alternatives, an analysis of scope and duration, consideration of the market power of the employer, and evidence of economic effects. Consistent with this policy, enforcement actions and similar initiatives are underway. The FTC most recently announced an enforcement action involving the alleged abuse of post-termination non-competes in violation of Section 5 on September 4, 2025.[66] And days later, the FTC issued warning letters to several health care employers and staffing firms urging them to conduct a comprehensive review of their employment agreements.[67] These actions signal that the FTC continues to work to restrict the scope and use of non-competes.

Federal Lawmakers Continue to Advance Legislation Seeking to Ban Non-Competes, but Passage Is Uncertain. On June 11, 2025, the Workforce Mobility Act of 2025, which seeks to ban non-competes with limited exceptions, was introduced in the Senate, continuing a pattern of legislative activity aiming to limit non-competes in prior sessions.[68] In fact, in 2023, a similar bill was introduced in the House and Senate but did not gain traction.[69] The reintroduced bill has some bipartisan support, and while it does not yet have a clear passage prospect as of

October 2025, the proposal signals sustained interest in limiting the use of non-competes at the federal level.

Practical Implications

Employers should continue to audit their non-compete agreements under the principles detailed in the FTC's recent statements and avoid using overly broad agreements. Further, employers should document why less restrictive alternatives to non-competes are inadequate to protect business interests.

State Developments

Legislative Activity Accelerates. Multiple states further tightened non-compete laws in 2025, continuing a multiyear trend. And several more introduced bills that, if passed, would significantly alter the non-compete landscape. Namely, Virginia passed legislation amending its non-compete law to expand the definition of "low-wage" employees to include all non-exempt employees.[70] Wyoming similarly banned most non-compete agreements with some exceptions.[71] Arkansas,[72] Louisiana,[73] Maryland,[74] Utah,[75] Oregon,[76] Montana,[77] Indiana,[78] Colorado,[79] and Pennsylvania[80] all passed legislation restricting non-competes among health care professionals. Furthermore, Michigan's HB 4040, Washington's HB 1155, Tennessee's SB 0995 and HB 1034, Ohio's SB 11, Texas's HB 4067, and New York's SB S4641 are all pending in their respective legislatures at various junctures in the process. Meanwhile, a number of other states have in place wage thresholds, duration caps, notice, and choice-of-law constraints to their non-compete laws.

Florida Goes Against the Trend Followed by Other States in Enacting Pro-Employer Legislation. On April 24, 2025, Florida passed the Contracts Honoring Opportunity, Investment, Confidentiality, and Economic Growth ("CHOICE") Act, which went into effect on July 3, 2025.[81] The Act applies to "covered employees," defined as employees or independent contractors who earn a base salary greater than twice the annual mean wage of the county where the employer's principal place of business is located, or where the employee resides in Florida if the employer is out of state. The Act extends the maximum enforcement period of a non-compete to four years and shifts the burden to the employee to show the agreement is unenforceable provided certain conditions are met. The Act also allows employers to enforce garden leave agreements for up to four years. It also provides for robust enforcement mechanism as it requires courts to preliminarily enjoin a covered employee from working for a competitor. Notably, any restrictive covenant agreements entered into prior to July 1, 2025, are governed by the existing law.

Choice-of-Law and Forum Restrictions Tighten. Following the lead of California and other jurisdictions limiting out-of-state choice-of-law/venue for employees who live and work locally, additional states in 2025 advanced or clarified anti-evasion rules. Notably, Florida's CHOICE Act specifies that it shall govern notwithstanding provisions of contrary law. This can create tension among competing state laws that each limit out-of-state choice of law. Expect more litigation over where a dispute can be heard and which law governs, particularly for remote and multistate employees.

Emerging Themes

The FTC is now focusing on targeted case-by-case enforcement actions. To bolster the likelihood that their non-competes and other restrictive covenants will survive these challenges, employers should be able to articulate a legitimate business interest for the scope and duration of restrictive covenants and tailor them to a particular geography, role, or industry.

There is also heightened invalidation risk and enforcement attention for low- and mid-wage workers, especially where income thresholds apply or where the restriction functionally forecloses employment in a field. Employers should consider whether non-competes are appropriate for these employee groups.

To protect business interests, companies may also implement trade-secret protection protocols such as access controls, need-to-know policies, exit interviews, and forensic audit capabilities to protect proprietary information without relying on non-competes.

Given the evolving and increasingly state-specific landscape for non-competes, employers with remote and multijurisdictional workforces should review agreements and tailor them by role and geography and consider addenda keyed to employee work location.

Restrictive covenants tied to the sale of a business remain the most defensible, but employers should review the specific state laws governing their employees to evaluate whether the sale-of-business exception applies.

Companies may also consider moving toward tiered protection models, such as role-based non-solicits and NDAs. To protect business interests, companies may also implement trade-secret protection protocols such as access controls, need-to-know policies, exit interviews, and forensic audit capabilities to protect proprietary information without relying on non-competes. Additionally, pre-hire and employee exit practices, such as clear notices, state-specific disclosures, and prompt return or deletion certifications, are becoming standard.

Action Items for 2026

Employers should take inventory of restrictive covenants by state, role, and compensation, and confirm each covenant's lawful basis, scope, and duration under the employee's work-state law. Agreements should be updated to implement role- and jurisdiction-specific non-solicits and NDAs, reserving non-competes for sale-of-business or permitted senior-executive contexts, and including state-required notices and wage floors.

Employers should be advised of the FTC's targeted enforcement priorities in light of its withdrawal of appeal in the circuit courts and continue to be mindful of state-by-state compliance as states update and amend their respective laws.

LAWYER CONTACTS

Randy Kay
San Diego/Silicon Valley
+1.858.314.1139/+1.650.739.3939
rekay@jonesday.com

Cary D. Sullivan
Irvine
+1.949.553.7513
carysullivan@jonesday.com

Margaret C. Gleason
Pittsburgh
+1.412.394.7235
mcgleason@jonesday.com

Andrea Weiss Jeffries
Los Angeles
+1.213.243.2176
ajeffries@jonesday.com

Steven M. Zadravecz
Irvine/Los Angeles
+1.949.553.7508/+1.213.243.2195
szadravecz@jonesday.com

Brent D. Knight
Chicago
+1.312.269.4290
bdknight@jonesday.com

Ryan K. Walsh
Atlanta
+1.404.581.8487
rkwalsh@jonesday.com

Michael A. Platt
Cleveland
+1.216.586.7221
maplatt@jonesday.com

Rick Bergstrom
San Diego
+1.858.314.1118
rjbergstrom@jonesday.com

Mark E. Earnest
Irvine
+1.949.553.7580
mearnest@jonesday.com

Jennifer D. Bennett
San Francisco
+1.415.626.3939
jenniferbennett@jonesday.com

The following lawyers contributed to this White Paper*: Joseph Chang, Lauren E. Dutkiewicz, Michael B. Gallagher, Kevin Ganley, Kyle Gantz, Nicholas Hodges, Rachel McKenzie, Alyssa M. Orellana, Matthew Rodriguez, Connor G. Scholes, and Kristen E. VandeVoort.*


KEY DEVELOPMENTS IN
CHINA

China's trade secret protection regime is undergoing sustained, meaningful reform. The newly amended Anti-Unfair Competition Law ("AUCL"), effective October 15, 2025, introduces greater flexibility in damage calculation and reinforces a trend toward higher compensatory and punitive awards. Courts have shown a growing willingness to grant robust interim relief, including pre-lawsuit preliminary injunctions in appropriate cases, and enforcement benefits from a coordinated "three-in-one" mechanism that aligns civil, criminal, and administrative tracks.

Together, these developments materially strengthen the position of trade secret owners in China.

INCREASED DAMAGES AND EXPANDED CALCULATION METHODS

Historically, damages in Chinese trade secret cases skewed low, constrained by evidentiary and methodological limitations. Over recent years, legislative changes and evolving judicial practice have addressed those constraints.

The 2019 AUCL amendment raised statutory damages from RMB 3 million to RMB 5 million and, critically, introduced punitive damages of up to five times the actual damages in trade secret matters.

Building on that foundation, the June 2025 amendment to the AUCL, effective October 15, 2025, clarifies and expands how damages may be assessed. Plaintiffs may now elect to calculate damages based on actual losses suffered or the improper profits obtained by the infringer, rather than relying on improper profits only where actual loss cannot be determined.

This added flexibility better aligns remedies with commercial reality and, in practice, should support larger and more predictable awards.

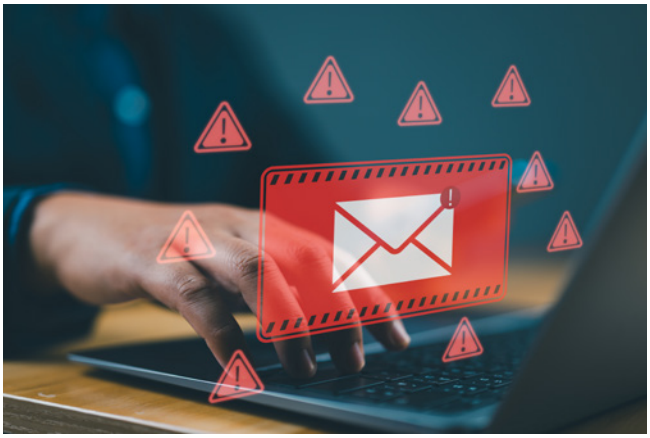
Courts have already signaled a readiness to impose higher damages under this framework.

In a December 2024 appeal before the Supreme People's Court, the court awarded RMB 166 million in total damages, including double punitive damages. The defendants—former employees who established competing operations during their employment—were found to have misappropriated software and foundational datasets for impeller models used in centrifugal compressor design and development.

Using the defendants' annual reports as a baseline, the court attributed roughly 30% of total profits to the misappropriated trade secrets and, noting the defendants' culpability, the severity of the infringement, and their refusal to cooperate with on-site inspections and evidentiary submissions, applied double punitive damages to post–April 2019 profits.

The decision underscores an emerging judicial willingness to deploy both compensatory and punitive tools to deter misappropriation and to capture the commercial value of stolen trade secrets.

PRE-LAWSUIT PRELIMINARY INJUNCTIONS



Because the disclosure of a trade secret can cause immediate and irreparable harm, rapid interim relief is essential.

Although Chinese judicial interpretations recognize imminent unlawful disclosure as a basis for a pre-lawsuit preliminary injunction, courts have traditionally approached such relief

with caution. Recent practice, however, evidences a measured openness to granting injunctions where the statutory framework is satisfied.

In July 2024, the Suzhou Intermediate People's Court granted Bosch a pre-lawsuit preliminary injunction to prevent a former employee from disclosing technical secrets that had been forwarded to a private email account in violation of confidentiality obligations.

Chinese courts apply a four-factor test in considering such relief: stability of the asserted right and likelihood of infringement; risk of irreparable harm to the right holder absent relief; the comparative balance of harms to the parties; and any impact on the public interest. For pre-lawsuit injunctions, courts must issue a decision within 48 hours.

In *Bosch*, the court convened a hearing and rendered a decision within one working day, finding a high likelihood of unauthorized disclosure and a compelling need to prevent further misappropriation.

The case, reported as the first pre-lawsuit preliminary injunction granted in a technical secret dispute, reflects the judiciary's growing commitment to swift and effective trade secret protection where the evidentiary record supports urgency and likelihood of success.

COORDINATED CIVIL, CRIMINAL, AND ADMINISTRATIVE ENFORCEMENT

China's three-track enforcement architecture—civil, criminal, and administrative—offers complementary pathways, each with distinct strengths and limitations.

Criminal filings have faced high thresholds for acceptance, historically requiring proof of actual losses or illicit gains exceeding RMB 300,000. Civil cases can be hampered by evidentiary challenges, particularly where misappropriation is covert. Administrative agencies, for their part, may lack technical depth in complex matters.

To address these frictions, authorities have implemented coordinated mechanisms that enable cases and evidence to flow among tracks, leveraging the investigative capabilities of public security bureaus, the remedial scope of courts, and the penalty powers of market supervision authorities.

In practice, administrative authorities can initiate investigations upon complaint and transfer suspected crimes to public security for criminal investigation. Conversely, public security can decline criminal acceptance where thresholds are unmet and refer matters to administrative regulators, who may impose penalties.

Evidence gathered in administrative or criminal proceedings can be used to support civil claims, improving plaintiffs' access to proof and reducing information asymmetries.

Localities such as Shanghai's Pudong New Area have formalized joint assessment protocols among market supervision departments, public security, and prosecutors to align investigative priorities and evidentiary standards early in a case, helping to direct rights holders toward the most effective remedy path.

One Shanghai case exemplifies this integrated approach: The Songjiang Market Supervision and Administration Department conducted an extensive administrative investigation and imposed RMB 1.5 million in penalties; the People's Procuratorate then brought criminal charges; and the rights holder pursued a civil action in the Shanghai Intellectual Property Court, which awarded RMB 2 million in damages.

The matter was recognized among Shanghai's "Top Ten Typical Cases of Trade Secrets Protection," illustrating the power of coordinated enforcement to deliver holistic protection.

LAWYER CONTACT

Haifeng Huang
Hong Kong/Beijing
+852.2526.6895/+86.10.5866.1111
hfhuang@jonesday.com

The following lawyers contributed to this White Paper*: Sophie Burgess, Jiahui Sheng, and Jessica Zhang.*


KEY DEVELOPMENTS IN
GERMANY

NEW POSSIBILITIES FOR COURT PROTECTION ORDERS IN (ALL) GERMAN CIVIL PROCEEDINGS

With the Justice Location Strengthening Act, enacted on April 1, 2025, the legislature has introduced § 273a of the German Code of Civil Procedure ("ZPO") as a general provision for the protection of trade secrets in all civil court proceedings. This closes a previous gap that existed because the respective provisions §§ 16 *et seq*. of the Company Secret Act (*GeschGehG*), which was enacted in 2019, apply only to proceedings where the trade secret is the subject matter of the dispute. In all other civil proceedings, there has been a lack of effective protection mechanisms for confidential company information.

Section 273a ZPO now allows the parties to have certain information classified as confidential by court order. This is not an automatic process, as the decision is within the court's discretion. The applicant must specify the information in detail and explain in a comprehensible manner why it is valuable and confidential information worthy of protection. General references to confidentiality are not sufficient. Rather, substantiated evidence showing reasonable measures of protection is required, proven, for example, by a confidentiality concept consisting of internal guidelines, trainings, technical access restrictions, confidentiality agreements, confidential communication, etc.

If the application is granted under § 273a ZPO, §§ 16 *et seq*. *GeschGehG* apply accordingly. This means that all parties involved in the proceedings—parties, proxies, witnesses, and experts—are obliged to treat the information subject to the court order confidentially. Use or disclosure outside the proceedings is prohibited (§ 16 (2) *GeschGehG*). Access to files by third parties may be restricted and, in particularly sensitive cases, even limited to a small group of people (§ 19 *GeschGehG*). Violations of confidentiality obligations are punishable by fines of up to €100,000 or administrative detention (§ 17 *GeschGehG*). The confidentiality obligations continue after the conclusion of the proceedings (§ 18 *GeschGehG*).

It is noteworthy that the new provision also applies to ongoing proceedings. This now gives courts a uniform instrument for effectively protecting trade secrets, regardless of whether the trade secrets are the subject matter or just a relevant aspect in proceedings based on other claims such as registered IP rights or contractual claims.

FEDERAL LABOR COURT, JUDGMENT OF OCTOBER 17, 2024 – 8 AZR 172/23

In a judgment dated October 17, 2024, the Federal Labor Court ("BAG") provided fundamental clarifications on the protection of trade secrets and the effectiveness of confidentiality clauses in employment contracts. The proceedings arose from a dispute between an employer and its former employee, who had provided technical data and process parameters to a potential competitor during the course of his employment. The employer considered this to be a serious breach of trade secret obligations and demanded that the employee refrain from passing on such information.

The Aachen Labor Court (judgment of January 13, 2022 – 8 Ca 1229/20) dismissed the action, arguing that the plaintiff had not sufficiently demonstrated that the data in question met the requirements of reasonable protection under the *GeschGehG*. The Cologne Regional Labor Court (judgment of September 28, 2022 – 11 Sa 128/22) upheld this decision

and found that there was a lack of adequate confidentiality management. The plaintiff's appeal to the BAG was also unsuccessful.

The BAG held that the plaintiff was unable to demonstrate "appropriate confidentiality measures" within the meaning of § 2 No. 1 b) *GeschGehG*. Although it referred to access controls and IT security measures, its submission remained too general to prove sufficient protection of the disputed technical data. Without verifiable appropriate protective measures, information cannot be considered a trade secret. The plaintiff was therefore not the "owner of a trade secret" within the meaning of the law and thus was not entitled to compensation under § 6 *GeschGehG*.

Only post-contractual confidentiality obligations that relate to clearly defined trade secrets and balance the interests of the employer and the employee are permissible.

In addition, the BAG declared the confidentiality clause contained in the employment contract to be invalid. This clause obliged the employee to maintain confidentiality about all internal matters of the employer—regardless of their substance or value—for an unlimited period of time. Such a broad and indefinite "catch-all clause" constituted an unreasonable disadvantage under § 307 (1) 1 of the German Civil Code prohibiting unfair Terms & Conditions. The BAG held it excessively restricted the employee's freedom of occupation, which is protected by Article 12 (1) of the German Basic Law, and was equivalent to a post-contractual non-compete clause without compensation for loss of earnings. Only post-contractual confidentiality obligations that relate to clearly defined trade secrets and balance the interests of the employer and the employee are permissible.

The ruling emphasizes the importance of structured management for the protection of trade secrets in companies. Only companies that can demonstrate concrete and appropriate measures to protect confidential information enjoy the legal protection of the *GeschGehG*. Blanket or unlimited confidentiality obligations do not meet these requirements and are generally invalid under German Law.

HIGHER REGIONAL COURT OF DÜSSELDORF, RULING OF NOVEMBER 14, 2024 – 2 U 17/24

The Higher Regional Court of Düsseldorf addressed whether a company being obliged by judgment to provide information and to render accounts due to a patent infringement may claim procedural secrecy protection under the *GeschGehG*. The defendant, a competitor of the plaintiff, sought to obtain a confidentiality order pursuant to §§ 16, 19 *GeschGehG* for the economic information to be disclosed under the plaintiff's successful claims for information due to the patent infringement.

The court rejected the application for trade secret protection. §§ 16 *et seq*. It held that *GeschGehG* did not apply to information to be disclosed as fulfillment of a judgment requiring such information to be provided and to render accounts. Under § 145a sentence 2 of the German Patent Act ("PatG"), the court ruled that the term "information in dispute" within the meaning of § 16(1) *GeschGehG* includes all information that either the plaintiff or the defendant has introduced into the proceedings. Information that is yet to be provided on the basis of a legally binding court decision does not fall within this category, as it is neither known nor part of the subject matter of the proceedings at the time of the decision.

The Higher Regional Court also rejected a derivation from the purpose limitation of the information data. The court held that any misuse could only be pursued by the party obliged to provide information retrospectively with claims for injunctive relief or damages. Although this purpose limitation reflects principles similar to those underpinning data protection law—particularly the EU General Data Protection Regulation's ("GDPR") principles of purpose limitation and data minimization—it does not in itself justify a separate procedural confidentiality

protection. The disclosure of sensitive company data to a direct competitor was not considered an exceptional but rather a typical consequence of the legal obligation to provide information in patent disputes. Ultimately, the court found that the protection of the injured party takes precedence over the infringer's interest in confidentiality.

The decision is not final; an appeal to the Federal Court of Justice is pending. § 145a PatG, which extends the confidentiality provisions of the *GeschGehG* to patent litigation, already provides a framework for protecting information disclosed in such proceedings. It therefore remains to be seen whether § 273a ZPO will be referred to in this context.

LAWYER CONTACT

Jakob Guhn
Düsseldorf
+49.211.5406.5500
jguhn@jonesday.com

The following lawyer contributed to this White Paper*: Larissa Brentrup.*

KEY DEVELOPMENTS IN FRANCE

TRADE SECRET PROTECTION UNDER FRENCH LAW

With the Law of July 30, 2018, France implemented the European directive of June 8, 2016, on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use, and disclosure. This law inserts new provisions into the French Commercial Code[82] that protect trade secrets from misappropriation.

REQUIREMENTS FOR TRADE SECRET PROTECTION

Three conditions must be met in order to benefit from trade secret protection: (i) the information must be secret; (ii) it must have commercial value; and (iii) reasonable protection measures must have been put in place in order to keep said information secret.

Several recent rulings, discussed below, provide valuable insight on the conditions under which courts recognize the existence of trade secrets, and on the remedies that trade secret owners can request in the event of breach.

Secret Information

Several court decisions illustrate what can and cannot constitute "secret information."

In its ruling issued on October 3, 2025, in the *École Polytechnique v. Matthieu Lequesne* case,[83] the French Supreme Court for administrative matters (*Conseil d'État*) held that sponsorship agreements can be secret information amounting to a trade secret. These documents are, depending on their degree of detail, likely to contain trade secrets, including economic and financial information, information related to the commercial or industrial strategies of these partner companies, foundations, or institutions, research in a specific field, or technical aspects of the projects in question.

Three other recent decisions held that information that was too general could not be considered "secret":

- The Paris First Instance Court held on January 31, 2025, in the *Arcoiris Studios GmbH v. Celine* case,[84] in relation to fashion photographic techniques, that claimants had not substantiated the existence of their alleged trade secrets, specifically in relation to the secrecy requirement, i.e., by providing clear, material, and specific evidence of the information for which they seek protection, rather than asserting vague and broad claims: "104. It is clear from the above list that these subcontractors, who are professional photographers, used common photographic techniques. Mr. [C] does not demonstrate that he invented the software reprocessing technique known as 'focus stacking,' which is used by the publisher of the software. He does not demonstrate that he has specific expertise, distinct from these techniques commonly used in the field of professional fashion photography, which should be protected as trade secrets. The existence of the aforementioned retouching tool is not demonstrated by any evidence. 105. Consequently, these elements, which are generally known and easily accessible to those familiar with the photography sector, do not constitute a trade secret."
- The Paris First Instance Court similarly recalled on February 21, 2025, in the *Soletanche Freyssinet v. Amtech* case,[85] in relation to a motorized arm used in nuclear facilities, that information relating to "an idea [or] the simple expression of a technical need" is unlikely to qualify as a trade secret.

- The Paris Court of Appeal on May 22, 2025, in the *Rolex v. Pellegrin & Fils* case,[86] considered that information that is more than five years old is rebuttably presumed to be no longer critical, unless its holder proves otherwise: "information that was secret or confidential but dates back five years or more must, due to the passage of time, be considered, in principle, as historical and, as such, no longer secret or confidential, unless, exceptionally, the party claiming such status demonstrates that, despite its age, this information still constitutes essential elements of its commercial position or that of third parties concerned." Given that the secrecy requirement must anyway be met regardless of time, the consequence of such case law seems to merely raise the bar for older trade secrets.

Commercial Value

Like for the secrecy requirement, commercial value must be specifically proven.

The Paris Court of Appeal in its ruling issued on September 10, 2025, in the *Domino's Pizza v. Speed Rabbit Pizza* case,[87] recalled that commercial value mainly depends on how current and relevant the information is: "The age of the compiled elements does not in itself deprive them of any commercial value, actual or potential, resulting solely from their secret nature, established in this case."

Also, in its ruling issued on May 27, 2025, in the *VPN France v. Weston NV* case,[88] the Bordeaux Court of Appeal found clear commercial value in "an Excel spreadsheet containing several hundred names of its used vehicle suppliers, with information for some of them such as intra-community VAT number, Credit Safe rating, and reference to creditworthiness assessments (with assessment date)," because "the distribution of this file, in a highly competitive market, had commercial value for Weston, giving it a complete overview of VPN France's regular suppliers, in a context of difficulties in sourcing used vehicles."

On the contrary, in its ruling issued on May 22, 2025, in the *Rolex v. Pellegrin & Fils* case,[89] the court held that Rolex did not specifically demonstrate why documents relating to the availability of watches had such commercial value.

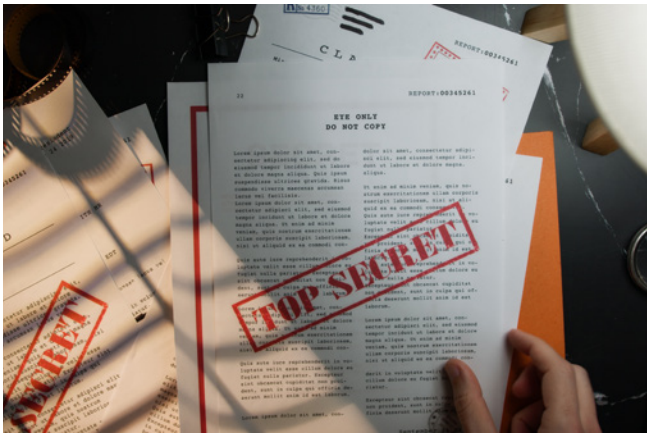
Reasonable Protection Measures

Protection measures must be reasonable, in light of the circumstances. As a general rule, "confidential" labels and limited or need-to-know distribution appear to be baseline protection measures that should meet the threshold set by courts in most cases.

Two recent cases held illustrate what constitute reasonable protection measures:

- The Bordeaux Court of Appeal in its ruling issued on May 27, 2025, in the *VPN France v. Weston NV* case,[90] noted that "[t]his file was sent to Mr. [C] by email on November 6, 2020, from Mr. [H] [D], audit and project manager at VPN Autos, with the subject line 'list of suppliers – CONFIDENTIAL' and marked 'Confidential' for distribution, which constituted a reasonable protective measure on the part of VPN France. (...) the VPN customer file, containing 3,463 contacts, and the VPN prospect file (11,615 contacts), each file containing names, company names, telephone numbers, and email addresses, for which the appellant did not have to take any special measures of secrecy, since the corresponding information had only been communicated to six VPN employees, respectively (email dated February 8, 2022)."
- The Paris Court of Appeal found, in its ruling issued on October 22, 2025, in the *Nanobiotix v. Ms. Sosse Alaoui* case,[91] that misappropriated technical documents, which related to the manufacturing process of a patented product, had been subject to reasonable protective measures by their legitimate owner, given the circumstances, namely: (i) the company's internal regulations contained confidentiality and discretion obligations, prohibiting any disclosure of confidential information and trade secrets, as well as the copying or transfer of computer files and documents; and (ii) the individual employment contracts also contained an explicit confidentiality clause. The court stressed that given that the product—to which the trade secrets related—was patented, the methods described above, used to maintain the secrecy of the manufacturing process, appeared reasonable in light of the circumstances.

UNLAWFUL ACT OF VIOLATION OF TRADE SECRETS



French law prohibits the unlawful acquisition, use, and disclosure of trade secrets.

Case law is now well-established regarding the fact that the mere possession of confidential information amounts to violation of trade secret, regardless of the lack of proof of actual use of the misappropriated information.

This case law was repeated by the Bordeaux Court of Appeal on May 27, 2025, in the *VPN France v. Weston NV* case[92]: "The possession and retention by Weston of this information, which constitutes trade secrets belonging to its competitor VPN France, constitutes a manifestly unlawful disturbance to which the judge hearing the application for interim relief had to put an end. In this regard, it is irrelevant that the plan to set up a subsidiary of VPN France in Hungary did not ultimately come to fruition and that the information relating to this plan was of no use or interest to Weston NV (. . .)."

This is confirmation of the principle set in three decisions of the French Supreme Court in 2022.

"The possession and retention by Weston of this information, which constitutes trade secrets belonging to its competitor VPN France, constitutes a manifestly unlawful disturbance to which the judge hearing the application for interim relief had to put an end.

EXCEPTIONS TO TRADE SECRET PROTECTION

Under Article L. 151-8 (3°) of the French Commercial Code, trade secrets are not enforceable when their acquisition, use, and disclosure of trade secrets is required "[f]or the protection of a legitimate interest recognized by European Union law or national law."

Right to Evidence

In its ruling of February 5, 2025, issued in the *Domino's Pizza v. Speed Rabbit Pizza* case,[93] the French Supreme Court recalled that a party may adduce a document during proceedings, even if it is protected by trade secrets, if that document is essential to prove the alleged facts (in this case, unfair competition) and if the infringement of trade secrets resulting from its obtaining or production is strictly proportionate to the objective pursued.

The Paris Court of Appeal applied this principle in two further rulings issued on September 10, 2025, in the same case,[94] but denied the exception for most documents for which it was raised, because their contents were not sufficiently necessary in order to support the arguments made by the infringer in the context of the proceedings. It upheld only the exception for the documents that actually supported the legal arguments made and where their use did not exceed the amount of information that needed to be disclosed for these purposes.

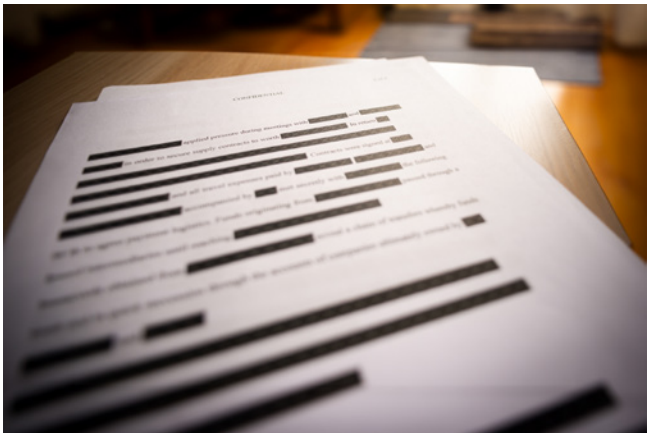
Interestingly, in its ruling issued on October 22, 2025, in the *Nanobiotix v. Ms. Sosse Alaoui* case,[95] the Paris Court of Appeal denied the right-to-evidence defense raised by an employee who had misappropriated technical documents,

because none of the documents unlawfully copied were actually relevant to or used in support of the action that the departing employee initiated against the former employer (which related to the classification of the employment contract, working hours, the obligation of safety, etc.).

Personal Data

The Court of Justice of the European Union ("CJEU") recently ruled that access to personal data under the GDPR is one of legitimate interest: In its ruling issued on February 27, 2025, in *CK v. Magistratder Stadt Wien* (C-203/22),[96] the court held that the fact that an automated decision-making software (here, related to the determination of a creditworthiness profile) may contain trade secrets does not prevent individuals whose personal data is processed by such software from exercising their data protection rights, by requesting access to "useful information concerning the underlying logic" of the software. However, through a balance between the right to protection of personal data with trade secrets and intellectual property, the CJEU held that when trade secrets are asserted, the data controller is required to disclose only the allegedly protected information to the competent supervisory authority or court, which is then responsible for balancing the rights and interests involved in order to determine the scope of the data subject's right of access under Article 15 of the GDPR, for example by granting limited access.

TRADE SECRETS AS AN EXCEPTION TO THE RIGHT OF ACCESS TO PUBLIC ADMINISTRATIVE DOCUMENTS



In principle, documents produced by a public law entity in the course of its public service mission are administrative documents that can be disclosed to persons who request them (in particular pursuant to Article L. 311-1 of the French Code of Relations between the Public and the Administration).

In its ruling issued on October 3, 2025, in the *École Polytechnique v. Matthieu Lequesne* case,[97] the French Supreme Court for administrative matters (*Conseil d'État*) held that trade secrets may constitute an exception to this principle, preventing such a request from being granted, for example when the request for disclosure concerns all contracts signed between a higher education public institution (in this case, the *École Polytechnique*) and its partner companies, foundations, or institutions for all chairs or sponsorship programs.

REMEDIES IN CASE OF TRADE SECRET BREACH

Judges can order several measures in case of violation of trade secret, first and foremost an injunction and damages.

Injunction and Destruction

In its ruling issued on October 22, 2025, in the *Nanobiotix v. Ms. Sosse Alaoui* case,[98] the Paris Court of Appeal found that shortly before her dismissal, an employee had misappropriated technical documents relating to the manufacturing process of a patented product, and the court ordered the following remedies:

- It prohibited the employee from using and disclosing the company's trade secrets to any third parties; and
- It ordered the employee to destroy any copies of the misappropriated trade secrets, at her cost and in the presence of a representative of the legitimate holder of the trade secrets, under the supervision of a judicial officer assisted, if need be, by any IT expert.

In a ruling handed down on February 21, 2025, by the Paris First Instance Court in the *Soletanche Freyssinet v. Amtech* case,[99] the court found that a measure for the preservation of evidence (*saisie-contrefaçon*) had resulted in the unlawful disclosure, to the adverse party, of numerous data files ("the 1,879 files seized, which are known to contain technical or accounting information relating to a product, the BMA152, resulting from a secret technical development and sold to a limited number of customers on a made-to-order basis, are therefore covered by trade secret protection"). The court thus ordered that party to destroy all copies of these documents in its possession (or in the possession of any third party to whom it may have given them) and to refrain from making any use thereof outside of a specific confidentiality club set up for the limited purpose of the proceedings.

Damages

In a ruling handed down by the Paris Court of Appeal on September 10, 2025, in the *Domino's Pizza v. Speed Rabbit Pizza* case,[100] the court found that the trade secret violation (in relation to the results of a market study) had resulted in substantive financial savings by the infringer, i.e., the cost of the misappropriated market study, and awarded €12,480 as damages based on the costs of such study, as well as €20,000 as moral damages. It refused to award damages based on the missed competitive advantage, loss of earnings, and loss of opportunity to optimize its sales that was claimed by the trade secret holder, however.

LOOKING AHEAD

With more and more trade secret violation cases being filed before French courts, case law continues to expand and develop nuances.

LAWYER CONTACT

Thomas Bouvet
Paris
+33.1.56.59.39.39
tbouvet@jonesday.com

The following lawyer contributed to this White Paper*: Colin Devinant*.


KEY DEVELOPMENTS IN
AUSTRALIA
CONFIDENTIAL
INFORMATION

GENERAL OBSERVATIONS AND TRENDS

In Australia, there is no general statutory regime that provides for the protection of trade secrets, nor are trade secrets considered to be proprietary in nature. However, there are a number of causes of action that can be brought for misuse of confidential information. These include breach of contract (where enforceable contractual provisions are in effect) and the equitable doctrine of breach of confidence. Trade secrets are one category of confidential information that can be protected through a breach of confidence action.

To establish a claim for breach of confidence, the claimant must:

- Identify the information in question with specificity;
- Establish that the information has the necessary quality of confidence;
- Establish that the information was imparted in circumstances by which an obligation of confidence was created; and
- Prove actual or threatened use or disclosure of the information without the claimant's consent.

As is the case in many other jurisdictions, a common context for a claim for misuse of confidential information in Australia relates to the use of such information by former employees. In these cases, some additional considerations arise under Australian law. Information developed by an employee during the course of employment may be considered to be "know-how," which may be used by the employee once the employment relationship ends (subject to any enforceable contractual restraint). Employees and executives may also be subject to equitable obligations arising from the fiduciary nature of the relationship between employer and employee/officer. Australian corporations legislation also prohibits the improper use of information by officers (including directors) and employees.

A party claiming that someone has misused its confidential information often faces difficulty in determining whether it has sufficient information to bring a claim for breach of confidence, or confronts the risk that key evidence may be destroyed if legal proceedings are commenced. There are a number of strategies available under Australian law to address these issues. For example, a party may seek an *ex parte* search (or "Anton Piller") order, or a preservation order, to address the risk that any evidence of breach may become unavailable in any legal proceedings. As well as the usual obligations of candor arising in the context of any *ex parte* application, there are significant hurdles to clear before such an order is granted given its invasive nature, and a number of safeguards are built into the terms of any order that is granted (including oversight by an independent lawyer).

If a party is concerned that its confidential information may have been misused, but does not have enough information to decide whether to bring a claim for breach of confidence, one option is to seek what is known as "preliminary discovery." This is an application for targeted discovery of key documents that is designed to enable the prospective applicant to decide whether it has sufficient grounds to commence substantive proceedings for breach of confidence.

Over many years, search orders and preliminary discovery applications have proven to be vital tools for any party concerned that its confidential information may have been misused by former employees, business partners, and/or other third parties. These tools recognize that one of the features of a claim for breach of confidence is that there are often difficulties in determining whether there has been a breach of confidence without access to non-public aspects of the alleged infringer's products (e.g., source code) and the alleged infringer's internal documents (e.g., documents relating to the development of its products).

DEVELOPMENTS IN 2025

In our 2024 update, we reported on the grant of *ex parte* search orders, and the subsequent application to set aside or vary those orders, in *Fortescue Limited v Element Zero Pty Limited (No 2)* [2024] FCA 1157. The application to set aside or vary the search orders was based in part on the fact that, in applying for those orders *ex parte*, Fortescue had failed to disclose to the court that Fortescue and Element Zero had an ongoing commercial relationship. This was asserted to be a breach of the duty of candor that (it was said) should result in the search orders being set aside.

In 2025, leave to appeal that decision was refused: *Element Zero Pty Ltd v Fortescue Ltd* [2025] FCA 206. The judge hearing the application for leave observed that the court retained discretion to refuse to set aside the search orders despite the material nondisclosure. One of the key factors in the exercise of that discretion was that there would be a lack of utility in granting leave to appeal, because the search orders had already been executed.

A fruitful line of defense in a breach of confidence action in Australia is to argue that the applicant has failed to adequately identify the allegedly confidential information (i.e., the first element of the cause of action noted above) and failed to establish that it is, in fact, confidential in nature (i.e., the second element of the cause of action). Two decisions published in 2025—*New Aim Pty Ltd v Leung (No 4)* [2025] FCA 747 (*New Aim v Leung*) and *Lift Shop Pty Ltd v Next Level Elevators Pty Ltd* [2025] FCAFC 108 (*Lift Shop v NLE*)—are illustrative of the difficulties faced by applicants in establishing these closely related aspects of the cause of action.

The first of these cases (*New Aim v Leung*) has had somewhat of a tortured history. It involved a company (New Aim) and one of its former employees (Jack Leung). The case was filed in 2021, a judgment at first instance in the Federal Court of Australia was handed down in 2022, and a decision on appeal was handed down in 2023. While appeals in the Federal Court are typically heard by three judges, an enlarged bench of five judges was assigned to hear this appeal, indicating that there were significant matters of principle to be determined. This likely related to the trial judge's decision to reject the entirety of the evidence of an expert witness engaged by New Aim, based on the manner in which the expert's written report was prepared. This was one of the (successful) grounds of appeal.

More relevantly for present purposes, the Full Court held that the trial judge erred in his approach to deciding whether the information in question was, in fact, confidential. The Full Court held that the trial judge had focused only on the location of the information and the way it was stored, and failed to properly consider the nature, substance, and commercial value of the information. The appeal court remitted the case for retrial.

The retrial was heard in 2024, with a decision handed down in 2025. New Aim is an e-commerce business that imports a broad range of products (principally from various suppliers in China), which it sells in Australia. By the time of his departure, Jack Leung was a senior New Aim employee. He had liaised with suppliers via WeChat on his personal cell phone, amassing a significant volume of New Aim supplier contact details. He retained this information following his departure from New Aim, and subsequently disclosed it to competitors of New Aim.

New Aim commenced proceedings against Leung and the competitors. New Aim alleged that the supplier information was confidential, and that it had gone to great efforts to carefully identify reliable and high-quality suppliers. Although the Federal Court acknowledged that such information was commercially valuable, it found that it did not have the necessary quality of confidence. The court considered the steps taken to guard the information, including that, for instance, New Aim employees were not provided with work phones and that employees were not required to delete such information following the termination of their employment. Furthermore, while it was not suggested that the information itself was generally known or available, the court reviewed submissions that

While it is not sufficient alone to mark a document with a confidentiality notice, this is important evidence that the "owner" of the document regards it as confidential, and it puts the recipient on notice of this fact.

supplier contact information may be publicly ascertainable, such as at industry events. Evidence was given that suppliers often disclosed or even advertised their relationships with New Aim. This latest decision has been appealed.

The second of these decisions (*Lift Shop v NLE*) primarily concerned a dispute between two competing suppliers of lifts, Lift Shop and Next Level Elevators ("NLE"). NLE had obtained a quotation issued to a customer by Lift Shop, and then adapted portions of it for its own use. The Lift Shop quotation (which was marked "Commercial-In-Confidence" in small print) contained terms and conditions, product specifications, and prices. The quotation had been uploaded to a tendering management platform and was made available for public access. Lift Shop commenced proceedings for breach of confidence, arguing that the quotation was confidential information when passed to the customer, and remained so when uploaded to the tendering management platform.

On appeal, the Full Court of the Federal Court of Australia did not accept Lift Shop's arguments, finding the assertion that the quotation was confidential had an "air of complete commercial unreality about it," particularly given that quotations are often intended as a basis for comparison with competing suppliers. The court noted that merely placing a confidential marking on a document does not make it so. Even if the quotation was confidential when first submitted to the customer, once it had been uploaded for public access (without the involvement of NLE), the Full Court held that it would be "absurd" to suggest that its contents remained confidential and that there would be any obligation of confidentiality on the part of NLE. Lift Shop's action for a breach of confidence against NLE therefore failed.

These cases illustrate the importance of safeguarding commercially sensitive information against misuse. While it is not sufficient alone to mark a document with a confidentiality notice, this is important evidence that the "owner" of the document regards it as confidential, and it puts the recipient on notice of this fact.

In an employment context, there are numerous steps that an employer should take to protect corporate confidential information. By way of example, employees should be instructed that confidential information is in fact confidential, appropriate access controls should be utilized, consideration should be given to whether (and, if so, how) information may be accessed on personal devices, there should be a requirement for employees to return or destroy confidential information in their possession at the time of their departure, and (importantly) compliance with that obligation should be monitored and enforced.

FEDERAL JURISDICTION AND STATUTORY DAMAGES

Traditionally, claims for breach of confidence in Australia were brought in the equitable jurisdiction of the various state courts. An increasing number of these cases are now brought in the Federal Court of Australia due to claimants asserting causes of action that create federal jurisdiction, such as copyright infringement and contraventions of corporations legislation. A copyright infringement claim can often be asserted in circumstances where a breach of confidence claim is brought (this was done in *Lift Shop v NLE*, for example). There are important strategic reasons for adding a copyright infringement claim: A claim of copyright infringement may entitle the claimant to additional statutory damages of a punitive nature not traditionally available in equity. Such damages may far exceed the actual loss suffered by the claimant.

PROPOSED BAN ON RESTRAINTS OF TRADE IN CERTAIN EMPLOYMENT CONTRACTS

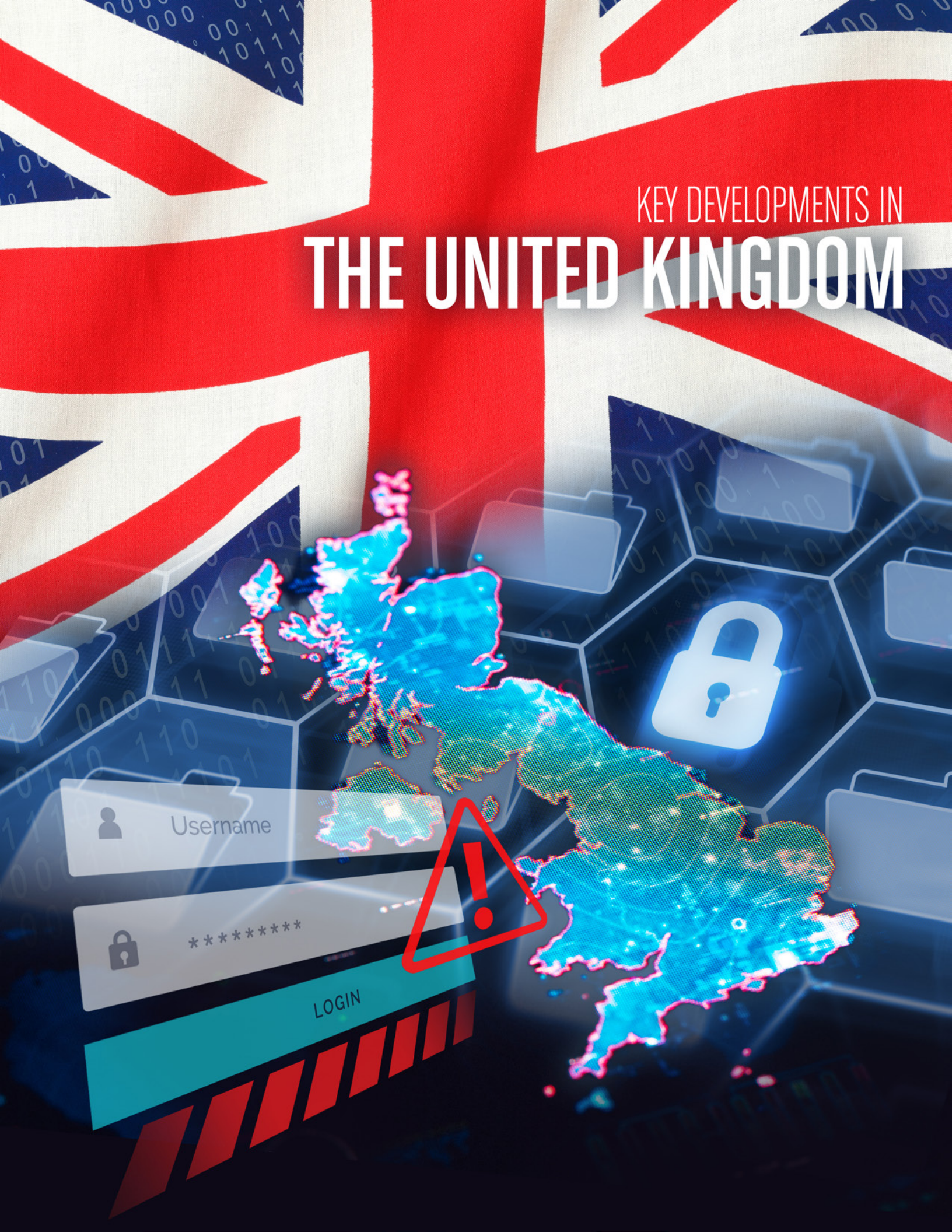
Earlier this year, the Australian government announced its intention to effectively ban non-compete clauses for employees under the high-income threshold stipulated in workplace legislation (currently AUD$183,100, although this figure is adjusted annually). These proposals would impact the vast majority of the Australian workforce, which would no longer be subject to post-employment restrictions that limit employees' ability to change jobs or start new businesses.

At present, these reforms are proposals only. A bill implementing the changes would need to pass both houses of the Federal Parliament before the ban could take effect. The government has announced that it intends these reforms to take effect in 2027. Businesses with operations in Australia should begin to assess their use of restraint clauses in Australia and ensure that employment contracts for individuals located in Australia include appropriately worded confidentiality clauses (as such obligations, it is hoped, will be unaffected by the ban).

LAWYER CONTACT

Richard Hoad
Melbourne
+61.3.9101.6800
rhoad@jonesday.com

The following lawyers contributed to this White Paper*: Harrison Cant and Emily Jennings.*


KEY DEVELOPMENTS IN
THE UNITED KINGDOM
Username
****
LOGIN

COURT OF APPEAL TIGHTENS "DIRECT DAMAGE" TEST FOR TRADE SECRET CLAIMS SERVED OUT OF THE JURISDICTION

Playtech Software Limited v Realtime SIA & Anor [2025] EWCA Civ 1472

Playtech Software Limited (the "claimant"), a company operating in the online gambling industry, brought claims for copyright infringement, breach of confidence, and misuse of trade secrets against several defendants. Initially, the claimant successfully demonstrated that its claims had a real prospect of success and was entitled to amend and to serve out of the jurisdiction in respect of those claims.

The claimant licensed online gambling games developed by its sister company, Euro Live Technologies SIA ("E") to operators of online gambling websites. The fifth defendant (Mr. Veliks) ("D5") had been employed by E to develop games and was given access to a software platform called Horizon. The Horizon platform hosts versions of games developed for the claimant, including both released and unreleased games. D5 then left his employment with E and was subsequently employed by Realtime SIA, the fourth defendant ("D4"), a Latvian company, to develop games. The claimant asserted that D5 continued to access the Horizon platform while employed by D4 (using login credentials from his previous employment). The claimant alleged that this conduct amounted to a breach of confidence, misuse of trade secrets, and infringement of copyright in the United Kingdom.

This appeal was brought by D4 and D5 on the grounds that the judge was wrong to find that the claimant suffered direct damage in the United Kingdom and that English law applies to the claim for alleged misuse of trade secrets. On the pleaded case, the alleged wrongful access and use occurred almost entirely in Latvia, and there was no allegation or evidence of UK downloads, access, or other UK-market acts causing direct damage. Loss of UK licensing revenues was an indirect consequence and insufficient to locate "damage" in the United Kingdom. Accordingly, Latvian law applied, and the claim did not pass Gateway 21 of paragraph 3.1 of CPR Practice Direction 6B, which the court held was the relevant jurisdictional gateway for breach of confidence claims, including claims for misuse of trade secrets—not Gateway 9, as relied upon by the first instance judge.

The court therefore set aside permission to serve the claim on the defendants outside the jurisdiction.

HIGH COURT GRANTS INTERIM INJUNCTIONS ENFORCING POST-TERMINATION RESTRICTIONS AND CONFIDENTIALITY OBLIGATIONS AGAINST FORMER EMPLOYEE AND COMPETITOR

United Kapital Limited v Favour Ayomide Bolaji, Sedulo Group Limited [2025] EWHC 1726 (KB)

Mr. Bolaji, the first defendant ("D1") had been employed by United Kapital Limited (the "claimant") as a funding specialist. The claimant is a company that provides alternative finance lending.

Post-termination restrictions in his employment contract prohibited him from exploiting or disclosing the claimant's confidential information post-termination, and for nine months after termination from being involved with named competitors of the

claimant, including Sedulo Group Limited, a financial services broker ("D2").

It also contained restrictions prohibiting D1 from working with competitors with whom he had been involved for the period of 12 months before his resignation, as well as non-deal and non-solicit restrictions for customers.

D1 resigned and began working for D2. The claimant alleged that D1 had passed confidential information about the claimant's clients to D2, including creating a spreadsheet of more than 850 of the claimant's customers and prospective customers, and included links to the claimant's internal records. D1 subsequently sent a mass marketing email to those customers included on the spreadsheet, informing them of his new employment with D2. D2 suspended D1 from employment.

The claimant further alleged that D1 continued breaching the post-termination restrictions after his suspension, including concluding four deals with contacts who had been included on the spreadsheet.

The court ordered D1 to return any documentation containing the confidential information, to deliver up any hard copies held, and not to publish or disclose any of the information. It also ordered D2 to give undertakings in relation to the protection of the confidential information, deliver up any of the information held, and not to permit D1 to resume his duties.

The claimant sought additional interim injunctive relief including:

- For D1 not to be involved without the claimant's consent with any person in competition with the claimant for a period of six months;
- Springboard relief that until judgment or further order D2 would not deal with any customer identified in a schedule to the order; and
- A restriction that D2 would not engage D1 in any capacity.

The claimant was granted the relief sought, the judge finding that D2 had secured an unfair head start through the use of information misappropriated by D1 from the claimant. The judge noted that the aim was to restore the parties to the competitive position they would have occupied had the defendants' breach not occurred. The court further concluded that damages would not constitute an adequate remedy for the claimant and that D1 was unlikely to be able to pay damages awarded at a trial. In those circumstances, it was held that the non-compete restrictions, though onerous, were necessary.

Finally, there have been no material legislative or regulatory changes in the United Kingdom in 2025, but we continue to monitor for any developments.

LAWYER CONTACT

Rebecca Swindells
London
+44.20.7039.5845
rswindells@jonesday.com

The following lawyer contributed to this White Paper*: Sophie Burgess*.

ENDNOTES

1 *Quintara Biosciences, Inc. v. Ruifeng Biztech, Inc.*, 149 F.4th 1081, 1085 (9th Cir. 2025).
2 *Id.* at 1086.
3 *Id.* at 1085.
4 *Id.* at 1089.
5 *Sysco Mach. Corp. v. DCS USA Corp.*, 143 F.4th 222, 227 (4th Cir. 2025).
6 *Id.*
7 *Id.* at 228–29.
8 *Id.* at 228.
9 *Id.*
10 *Id.* at 228–29.
11 *Id.* at 229 (quoting *Krawiec v. Manly*, 811 S.E.2d 542, 548 (N.C. 2018)).
12 *Id.*
13 *Id.* at 230.
14 *Id.*
15 *Samuel Sherbrooke Corp. Ltd v. Mayer*, 149 F.4th 252, 254–55 (4th Cir. 2025).
16 *Id.* at 255.
17 *Sherbrooke Corp. Ltd v. Mayer*, No. 24-cv-57, 2024 WL 4557318, at *3 (E.D.N.C. Oct. 23, 2024).
18 *Id.* at *4.
19 *Sherbrooke Corp. Ltd v. Mayer*, 149 F.4th at 259.
20 *Id.* at 257.
21 *Id.*
22 *Id.* at 256.
23 *Id.* at 258.
24 *NRA Grp., LLC v. Durenleau*, 154 F.4th 153, 160–61 (3d Cir. 2025).
25 *Id.* at 171.
26 *Id.* at 171.
27 *Id.* at 170–171.
28 *Id.* at 172.
29 *Id.* at 171.
30 *Id.* at 172.
31 *Id.* at 171.
32 *Id.*
33 *Id.*
34 *PleasrDAO v. Shkreli*, No. 24-cv-4126, 2025 WL 2733345, at *11 (E.D.N.Y. Sep. 25, 2025).
35 *Id.* at *8.
36 *Id.* at *10.
37 *Id.*
38 *Double Eagle Alloys, Inc. v. Hooper*, 134 F.4th 1078, 1099–100 (10th Cir. 2025).
39 *Id.* at 1100.
40 *Id.* at 1089.
41 *Id.* at 1091.
42 *Id.*
43 *Id.* at 1093.
44 *Id.*
45 *Id.* at 1096.
46 *Id.*
47 *Id.* at 1096–97.
48 *Id.* at 1097.
49 *Harbor Bus. Compliance Corp. v. Firstbase.io, Inc.*, 152 F.4th 516, 531 (3d Cir. 2025).
50 *Id.*
51 *Id.*
52 *Id.* (citation modified) (quoting *Oakwood Labs. LLC v. Thanoo*, 999 F.3d 892, 912 n.19 (3d Cir. 2021)).
53 *Id.* at 531–32.
54 *Id.* at 535–37.
55 *Id.* at 536.
56 *Id.*
57 *Id.*
58 *Id.* at 537.
59 *Id.*
60 *Id.* at 134, 136.
61 *Id.* at 136–37.
62 *Id.* at 136.
63 *Id.* at 139–40.
64 *Federal Trade Commission Files to Accede to Vacatur of Non-Compete Clause Rule*, Fed. Trade Comm'n (Sep. 5, 2025).
65 15 U.S.C. § 45(a).
66 Andrew N. Ferguson & Melissa Holyoak, *Statement of Chairman Andrew N. Ferguson Joined by Commissioner Melissa Holyoak In the Matter of Gateway Pet Memorial Services*, Fed. Trade Comm'n (Sep. 4, 2025).
67 *FTC Chairman Ferguson Issues Noncompete Warning Letters to Healthcare Employers and Staffing Companies*, Fed. Trade Comm'n (Sep. 10, 2025).
68 Workforce Mobility Act of 2025, S. 2031, 119th Congr. (2025).
69 Workforce Mobility Act of 2023, H.R. 731, 118th Congr. (2023); Workforce Mobility Act of 2023, S. 220, 118th Congr. (2023).
70 2025 Va. Acts Ch. 585.
71 Wyo. Stat. § 1-23-108 (2025).
72 2025 Ark. Acts 232 (S.B. 139).
73 2024 La. Act 273 (S.B. 165).
74 H.B. 1388, 2024 Gen. Assemb., Reg. Sess. (Md. 2024).
75 S.B. 228, 2025 Gen. Sess. (Utah 2025).
76 S.B. 951, 2025 Reg. Sess. (Or. 2025).
77 H.B. 198, 69th Leg., 2025 Reg. Sess. (Mont. 2025); H.B. 620, 69th Leg., 2025 Reg. Sess. (Mont. 2025).
78 S.B. 475, 124 Gen. Assemb., 2025 Reg. Sess. (Ind. 2025).
79 S.B. 83, 2025 Reg. Sess. (Colo. 2025).
80 2024 Pa. Legis. Serv. Act 2024-74 (H.B. 1633) (West).
81 H.B. 1219, 2025 Reg. Sess. (Fla. 2025).
82 Articles L. 151-1 *et seq.* of the French Commercial Code.
83 French Supreme Court for administrative matters (*Conseil d'État*), Oct. 3, 2025, *École Polytechnique v. Matthieu Lequesne*, Docket No 490433.
84 Paris First Instance Court, Jan. 31, 2025, *Arcoiris Studios GmbH v. Celine*, Docket No 21/13754.
85 Paris First Instance Court, Feb. 21, 2025, *Soletanche Freyssinet v. Amtech*, Docket No 22/12080.
86 Paris Court of Appeal, May 22, 2025, *Rolex v. Pellegrin & Fils*, Docket No 24/03052.
87 Paris Court of Appeal, Sep. 10, 2025, *Domino's Pizza v. Speed Rabbit Pizza*, Docket No 23/02282.
88 Bordeaux Court of Appeal, May 27, 2025, *VPN France v. Weston NV*, Docket No 23/03277.
89 Paris Court of Appeal, May 22, 2025, *Rolex v. Pellegrin & Fils*, Docket No 24/03052.
90 Bordeaux Court of Appeal, May 27, 2025, *VPN France v. Weston NV*, Docket No 23/03277.
91 Paris Court of Appeal, Oct. 22, 2025, *Nanobiotix v. Ms. Sosse Alaoui*, Docket No 22/04555.

92 Bordeaux Court of Appeal, May 27, 2025, *VPN France v. Weston NV*, Docket No 23/03277.

93 French Supreme Court, Feb. 5, 2025, *Domino's Pizza v. Speed Rabbit Pizza*, Docket No 23-10.953.

94 Paris Court of Appeal, Sep. 10, 2025, *Domino's Pizza v. Speed Rabbit Pizza*, Docket No 23/02449 and 23/02282.

95 Paris Court of Appeal, Oct. 22, 2025, *Nanobiotix v. Ms. Sosse Alaoui*, Docket No 22/04555.

96 CJEU, Feb. 27, 2025, *CK v. Magistratder Stadt Wien* (C-203/22).

97 French Supreme Court for administrative matters (*Conseil d'État*), Oct. 3, 2025, *École Polytechnique v. Matthieu Lequesne*, Docket No 490433.

98 Paris Court of Appeal, Oct. 22, 2025, *Nanobiotix v. Ms. Sosse Alaoui*, Docket No 22/04555.

99 Paris First Instance Court, Feb. 21, 2025, *Soletanche Freyssinet v. Amtech*, Docket No 22/12080.

100 Paris Court of Appeal, Sep. 10, 2025, *Domino's Pizza v. Speed Rabbit Pizza*, Docket No 23/02449 and 23/02282.