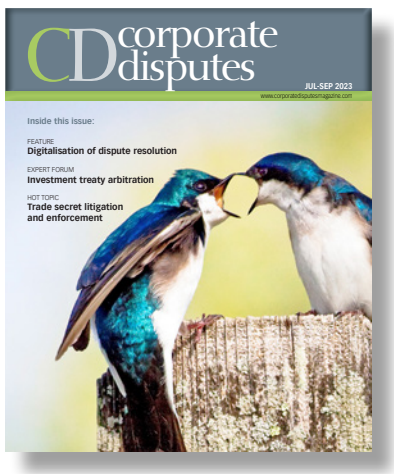
REPRINT

CD corporate disputes

TRADE SECRET LITIGATION AND ENFORCEMENT

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
JUL-SEP 2023 ISSUE



www.corporatedisputesmagazine.com

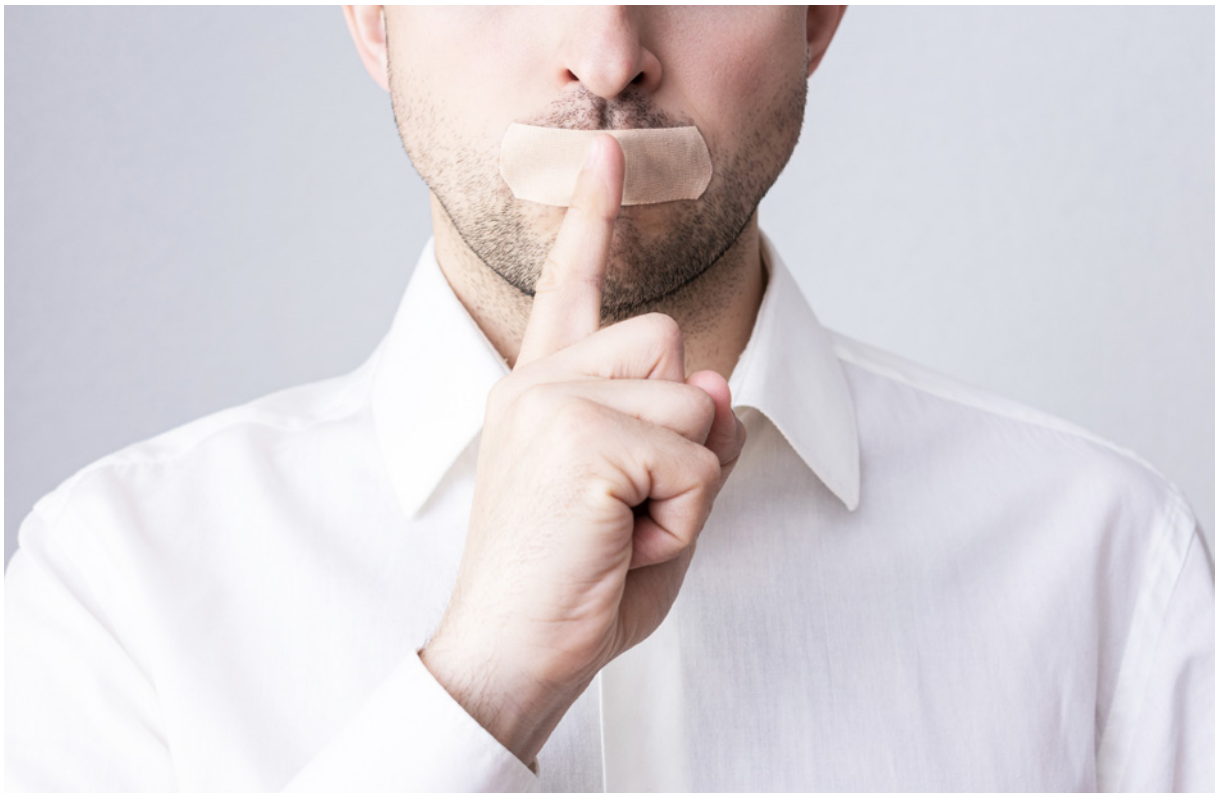
Visit the website to request a free copy of the full e-magazine

LATHAM & WATKINS LLP

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

HOT TOPIC

TRADE SECRET LITIGATION AND ENFORCEMENT



PANEL EXPERTS

Rogier de Vrey
Partner
CMS
T: +31 20 301 62 59
E: rogier.devrey@cms-dsb.com

Rogier de Vrey is a partner in CMS's Amsterdam office and chair of the firm's intellectual property practice. He has extensive experience in all aspects of IP and media & advertising matters, advising well-known companies in the field of technology, media, communications and life sciences. He is a Domain Name Panelist (arbiter) at the WIPO, associate professor at the Utrecht University and member of one of the leading Dutch journals covering IP and unfair competition law.

Jeff Homrig
Partner
Latham & Watkins LLP
T: +1 (737) 910 7344
E: jeff.homrig@lw.com

Jeff Homrig is a seasoned first-chair trial lawyer who handles complex and high-stakes intellectual property and commercial cases around the country for some of the world's most innovative technology and life sciences companies. He serves as vice chair of Latham's intellectual property litigation practice and previously chaired the Silicon Valley and Bay Area litigation & trial departments.

Rachel E. Epstein
Partner
Quinn Emanuel Urquhart & Sullivan, LLP
T: +1 (212) 849 7485
E: rachelepstein@quinnemanuel.com

Rachel E. Epstein is a partner in Quinn Emanuel's New York office and co-chair of the firm's trademark, copyright and trade secret practices. She is an experienced litigator with a focus on complex commercial litigation and international arbitration across all industries, including technology, entertainment, insurance, energy and financial institutions. She has an active trial practice as both plaintiff and defence counsel, and has had leading roles in numerous trials and arbitrations, including intellectual property, licensing, technology and media, and entertainment disputes.

James Y. Pak
Counsel
Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates
T: +1 (650) 470 3197
E: james.pak@skadden.com

James Y. Pak focuses his practice on litigating intellectual property matters, including patent infringement, copyright infringement and trade secret misappropriation. He also counsels companies on acquiring, evaluating, licensing and protecting intellectual property assets. Mr Pak has significant experience representing companies on matters involving complex technologies, including computer source code, wireless communications, data messaging, storage systems, databases, digital imaging, computer graphics, encryption and virtual reality.

CD: Could you provide an overview of why trade secrets are so important to many companies?

de Vrey: The protection of trade secrets covers a broad range of information. For example, it can refer to technological knowledge and commercial information. Now that big data is considered to be one of the most valuable 'assets' in commerce these days, the possibility for protection under trade secret law is valuable, as current intellectual property (IP) laws often do not provide sufficient protection. Trade secrets can be a highly valuable asset to a company. Trade secrets support the innovation ecosystem by protecting process, product, market and organisational innovations. In contrast to other IP rights, trade secrets do not involve disclosure. The period of protection is as long as secrecy is maintained. Using trade secrets is usually cheaper than using IP rights because trade secrets do not have to be registered. Registering IP rights is usually a very costly process. This can be a huge asset for small and medium-sized enterprises (SMEs) that do not always have the money for patent applications, for example.

Pak: Trade secrets are often referred to as the 'crown jewels' of a company and there is a reason for that. Most trade secrets are developed through extensive research that comes at a significant cost both in terms of time and money. And once that time and money are invested, those trade secrets can give companies a real competitive edge – a secret manufacturing process, technology blueprint, computer source code or other information that competitors are not aware of and cannot benefit from. So, it is important that once those trade secrets are developed and have substantial value, they are protected from disclosure.

Epstein: In a rapidly evolving global economy that prizes innovation, trade secrets are vital to a company's ability to expand and maintain its competitive position. Trade secrets such as computer algorithms, manufacturing processes or a company's 'secret sauce' are often worth billions of dollars and may even be a company's most valuable asset. Furthermore, trade secret protection extends to a wide range of subject matter, including customer lists and marketing strategies, that are not covered by other intellectual property schemes such as patents. And unlike other forms of IP, trade secrets enjoy perpetual protection so long as companies take reasonable measures to safeguard them from unauthorised use, acquisition or disclosure.

Homrig: For many companies, trade secrets reflect the company's core value – what differentiates it from its competitors and makes its products and services attractive to customers. That

is certainly true in the technology space, where many innovators are reluctant to divulge their most important advances in patents, which require a detailed public disclosure of the invention, or find that their key innovations are not patent-eligible. It is also true outside the technical sphere. So often, a company's business strategies, customer analytics and target analysis, pricing information and strategies, manufacturing processes or supplier lists and information provide the critical edge to win business and drive profits. If a company plays its cards right, all of these categories of information are protectable as trade secrets.

"In making a determination as to whether certain information is a trade secret, the law often examines the conduct of the company that owns that information."

James Y. Pak, Skadden, Arps, Slate, Meagher & Flom LLP and Affiliates

CD: How prevalent is the misappropriation of trade secrets in today's business world? Do you believe companies are sufficiently aware of the risks?

Pak: It is almost a given at this point that employees will work at several companies over their career, especially in Silicon Valley. And with that movement from company to company there is always a risk that trade secrets and other IP will be improperly taken or used by an employee or former employee, intentionally or not. Sometimes trade secret misappropriation is suspected immediately, while other times it is only suspected later, such as after the announcement of new technology from a competitor. I think companies are aware of this risk, but there is always more that can be done to minimise the risk and ensure that policies are continuously reviewed and enforced.

Epstein: The digitalisation of IP and information places companies at an elevated risk of trade secret misappropriation. Today, companies face a highly competitive business environment in which it is both easier to access trade secrets without authorisation and harder to 'stop the bleeding' once data is exfiltrated. Despite a growing incidence of trade secret misappropriation, most companies are largely unprepared to safeguard their trade secrets,

whether against outside threats, such as hacking and other forms of unauthorised downloading, or internal threats, such as dissatisfied or exiting employees. However, the private sector is becoming increasingly aware of the enhanced threat of trade secret misappropriation and the enormous costs associated with failing to invest sufficiently in procedures to safeguard them.

Homrig: Trade secret misappropriation is most often triggered by one of two events: an employee moves companies, or one company meets with another to discuss a business deal, be it an acquisition, investment, partnership or the like. With employee mobility at record levels, the risk of trade secret misappropriation is very high. And when the business climate improves, increasing investment and deal flow, that risk will only increase. Importantly, this risk goes both directions, with every employee who leaves and every employee who joins, bringing the risk of trade secret misappropriation. To a large extent, the same is true for business discussions. Savvy companies know this, stay vigilant and prepare both to protect their trade secrets and to defend themselves against claims of trade secret misappropriation.

de Vrey: In today's business world, the misappropriation of trade secrets is becoming more common. Misappropriation can take many forms, including breaches of non-disclosure agreements (NDAs), industrial espionage and theft. The latter is becoming more common with the increasing number of cyber attacks. Both commercially, for example in the high-tech industries sector, but also geopolitically, the world has been increasingly confronted with cases of misappropriation of valuable trade secrets. Therefore, it cannot be overemphasised that companies must protect their trade secrets and implement steps to mitigate the risks. Many companies are aware of the risks. However, there are also many companies that have a general lack of awareness of the threat posed by the theft of trade secrets and the measures that should

"Trade secret information is becoming increasingly valuable as companies rely on proprietary technology, algorithms and other confidential information to gain a competitive edge."

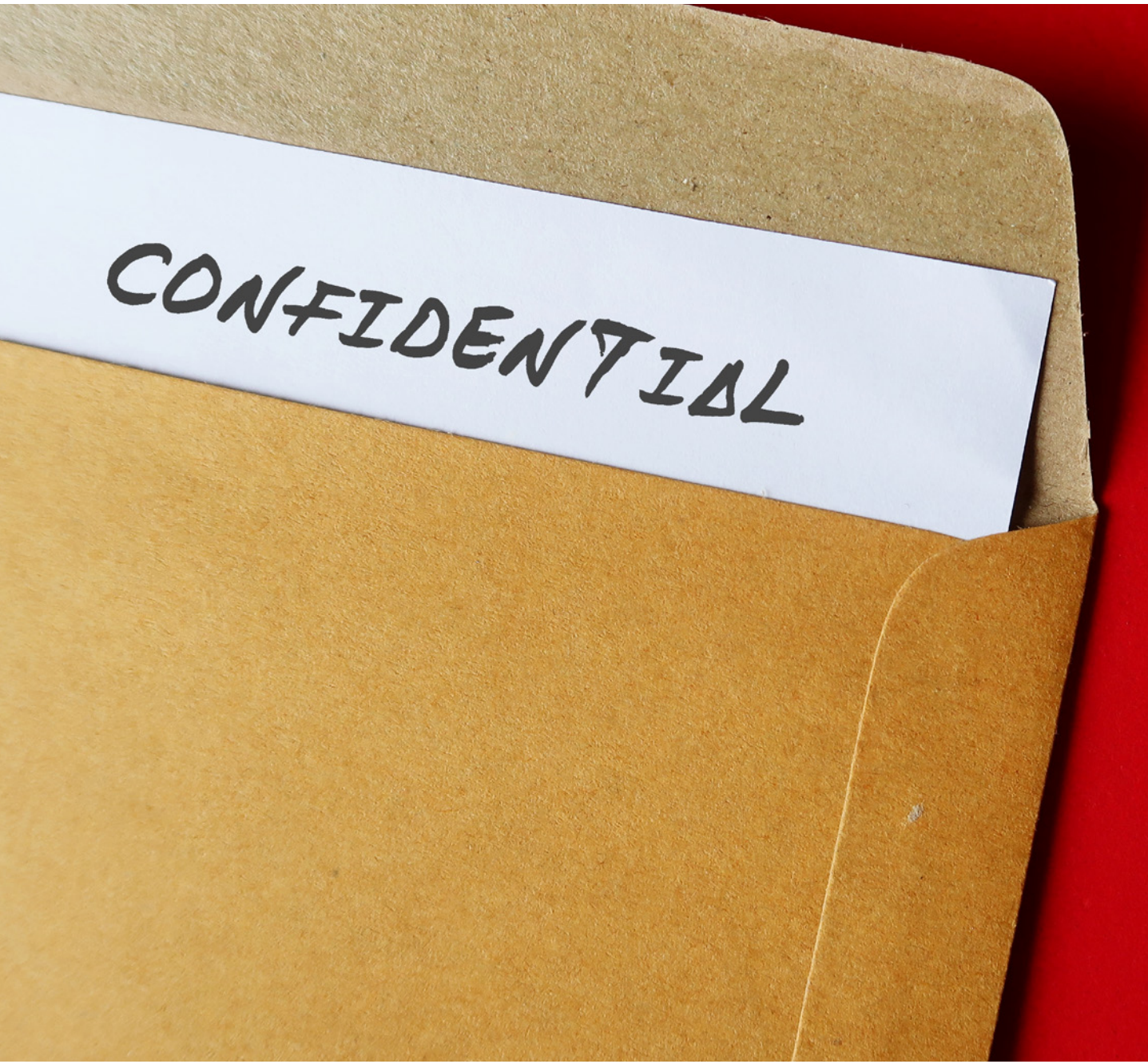
Rachel E. Epstein, Quinn Emanuel Urquhart & Sullivan, LLP

be put in place to prevent it. The consequences of misappropriation of trade secrets can be disastrous to the company. The consequences could be loss of market share, reputational damage and loss of customer trust.

CD: What essential steps should companies take in order to protect their trade secrets? What are the potential consequences of failing to safeguard proprietary information?

Epstein: Companies should put greater emphasis on the basic step of identifying their trade secrets. This may include marking documents 'confidential' as well as developing confidentiality policies, employee training and contractual terms that make employees, consultants and third parties aware of what information must not be disclosed without authorisation. Companies should pay careful attention to any exchange of information pursuant to contract, and any marking requirements therein. From a technological perspective, companies should bolster their investments in information security, including the use of secure servers and videoconferencing platforms to save and communicate sensitive company information. The consequences of failing to safeguard trade secrets can be devastating. As with other types of innovation, if a company spends billions of dollars developing trade secrets and is then unable to obtain a profit or competitive advantage, this can have catastrophic financial consequences. It may also cause additional harm such as reputational damage, disruption to operations, and decreased incentive to innovate. And when companies fail to take reasonable measures to protect their proprietary information, courts often find that their information has lost trade secret status.

de Vrey: Companies should take steps to safeguard their trade secrets. As threats come in many forms, both internal and external, it is imperative to develop best practices for protection. Technical and business management and legal counsel should identify trade secrets and develop a plan to protect them. Companies should revisit these plans regularly and at every important moment in the company life cycle. In the end, a company must be able to provide evidence that it has taken sufficient measures on a legal, technical and organisational scale to ensure that is has done everything needed to keep information secret. Furthermore, a trade secret owner should use a well-drafted NDA. NDAs are advisable for everyone coming into contact with trade secrets. Finally, companies should have a contingency plan and know what to do when harm is done. The potential consequences of failing to safeguard proprietary information correctly could be disastrous. In a legal


CONFIDENTIAL

case, the court will probably dismiss the plaintiff's claim because the plaintiff has failed to properly protect the trade secrets concerned, because the plaintiff has not taken sufficient measures to keep the data secret.

Homrig: First and foremost, companies should protect their trade secrets by treating them as secret: implement internal controls, compartmentalise access to key information, identify what is secret and communicate that fact to employees, require NDAs for business meetings, and implement sophisticated IT and forensic capabilities. Each of these steps helps prevent theft and prepares the company to act quickly when theft occurs. Implementing onboarding and offboarding procedures that manage trade secret risk is vital. Of course, employment-contract provisions establishing the company's ownership of confidential information and restrictions on its use and dissemination, along with provisions barring the use of confidential information from prior employers, provide a critical foundation, but they are not enough. When joining, employees should be asked, in a separate document that is simple and easy to read, to acknowledge these obligations and promise to uphold them. When leaving, employees should be asked to sign a similar document stating that they have returned all company information, do not have company information on their personal devices, and will not use the company's confidential information. These simple steps achieve two equally important goals, namely dissuading the employee from wrongdoing and creating a record that will prove critical if a dispute arises.

Pak: Companies should coordinate with all relevant stakeholders, including management, IT, HR and legal, to establish a comprehensive policy to protect trade secrets and other confidential information. The policy should look at how trade secrets are identified, protected and disclosed to both employees and third parties. What information should be protected? What steps must be taken to identify and distinguish that information? What confidentiality agreements and NDAs must be in place? Who at the company will be entitled to access that information? The policy should also outline how new employees will be onboarded, and how departing employees will be exited. What questions and instructions will those employees be given? What documents will they sign? The policy must also be regularly reviewed and revised to appropriately reflect any changes within the company. And most importantly, the policy must be enforced at all levels and departments of the company.

CD: What actions and remedies are available to companies whose trade secrets have been misappropriated?

Could you outline any recent legal or regulatory developments in this area?

Homrig: In the US, the Defend Trade Secrets Act (DTSA) provides a nationwide framework for addressing trade secret misappropriation, including both criminal prosecution and private civil litigation. While individual state laws remain available, the DTSA, which was enacted in 2016, is now the vehicle of choice for most private litigants when bringing significant trade secret enforcement actions. Importantly, the DTSA encompasses conduct worldwide, so long as the misappropriation affects US commerce. In other words, if the product or service resulting from the misappropriation is sold in the US, the misappropriation is actionable in US courts under the DTSA even if that misappropriation occurred outside the US. Another recent development is the emergence of the US International Trade Commission (ITC) as a venue for trade secret enforcement. Long a venue for patent infringement claims because of its power to bar products from the US market, the ITC typically acts more quickly than US courts and its exclusion orders are enforced by US Customs and Border Protection. Consequently, it provides a powerful option for enforcement when products arising from the misappropriation are being imported into the US.

Pak: The most common civil action in the US is a claim for trade secret misappropriation under either the federal DTSA or state trade secret law. Another common action is a claim for violation of the Computer Fraud and Abuse Act (CFAA). The CFAA provides for a civil remedy when there has been wrongful access of certain protected computer systems. And other IP claims such as copyright or patent infringement should also be considered. In addition to the claims above, a company should consider seeking injunctive relief. In the typical case, this involves asking a court to restrain an individual or company from further using or disclosing the information at issue, either on a temporary or permanent basis. This is usually requested in order to limit further harm to the company and prevent the trade secret from becoming more widely known and thus less protectable under trade secret law.

de Vrey: Under Dutch law, the measures and remedies that are available in the event of infringement of trade secrets are listed in the Trade Secret Act, the implementation of the European Trade Secret Directive. The trade secret holder can request the court to order the following interim or final measures. First, cease and desist use or disclosure of the trade secret. Second, prohibit infringing goods from being produced, offered, placed on the market, or used, imported, exported or stored. Third, seize infringing goods. Fourth, recall

infringing goods. Fifth, deprive infringing goods of their infringing quality. Sixth, destroy infringing goods or withdraw them from the market, provided that the withdrawal does not undermine the protection of the trade secret in question. Finally, destroy all or part of any document, object, substance, material or electronic file containing the trade secret.

Epstein: Companies routinely bring trade secret misappropriation claims to enjoin the actual or threatened misappropriation of their trade secrets. In the US, plaintiffs bringing such claims have several damages theories at their disposal, including recovery of lost profits, disgorgement of the defendant's profits attributable to the misappropriation and a 'reasonable royalty' consisting of the amount the defendant would have paid if it had fairly bargained for a licence to use the trade secret. In addition, in certain states, companies may have additional remedies against employees who steal trade secrets, including disgorgement of any compensation those employees received. In recent years, courts have increasingly recognised another damages theory known as 'avoided costs'. Under this theory, a plaintiff can recover the amount that the defendant saved, including research and development costs, as a result of misappropriating its trade secret. The 'avoided costs' theory has led juries to award damages approaching or exceeding a billion dollars. Crucially, it has also enabled plaintiffs to prove damages that may otherwise have been impossible to prove.

> **"One of the most challenging aspects of effective trade secret protection is balancing risk management with company culture."**
>
> *Jeff Homrig, Latham & Watkins LLP*

CD: In the event of pending litigation, how should companies go about preparing their case and asserting their rights?

Pak: When companies suspect trade secret misappropriation, they should move quickly to conduct an investigation and take legal action as soon as they have a basis for doing so. Otherwise, they risk losing those trade secrets through further disclosure. In fact, in making a determination as to

whether certain information is a trade secret, the law often examines the conduct of the company that owns that information. If the company has shown a consistent pattern of proactively protecting its confidential information and investigating potential claims that the information was misappropriated, then the law is more likely to find that information subject to trade secret protection as well.

de Vrey: Companies should be able to clearly define the trade secrets concerned. An inability or unwillingness to articulate one's trade secrets will damage the plaintiff's credibility. Furthermore, companies should be able to show the court that reasonable measures were taken to keep the information safe. In the event of pending litigation, companies should always gather evidence regarding the misappropriation of the trade secret. To gather and preserve evidence of infringement of trade secrets, the trade secrets' owner can request a prejudgment seizure of evidence of infringement of trade secrets. Finally, the trade secret holder can ask the court to introduce a so-called 'confidentiality club'. Dutch courts can determine that access to alleged trade secrets introduced in the proceedings is only granted to at least one person of the opposing party and that party's lawyer under confidentiality restrictions.

Epstein: As soon as a company identifies that trade secret misappropriation has occurred, the company should conduct a prompt and thorough pre-litigation investigation to determine precisely what information has been misappropriated and by whom. It is critical to identify, for instance, whether a former employee stole trade secrets on their own initiative or at the request of their new employer. Given that trade secret litigation can be quite complex, companies should retain outside legal counsel early on. Counsel experienced in trade secret law can advise companies on how best to avoid litigation, such as by sending a cease-and-desist letter to the individual or organisation behind the misappropriation which identifies the appropriated material and demands its immediate

> **"Innovation is one of the core principles of doing business in a globalised world and trade secrets are essential for innovation."**
>
> *Rogier de Vrey, CMS*

return. If, however, litigation appears inevitable, companies should consult with counsel regarding what measures were taken to maintain the secrecy of the information in question, as well as the value that information provided to the company by not being publicly known.

Homrig: Companies should be proactive, deliberate and involve the IT team from the outset. At the first sign of a trade secret problem, they should engage with the legal team, direct IT to implement controls to prevent the further loss or, in the case of inbound material, spread of confidential material, and where appropriate forensically preserve relevant data, and begin to gather and organise the relevant documents, such as employment agreements, onboarding and offboarding materials and NDAs. It is prudent to pause to assess legal strategy and business goals before contacting or responding to the individual or company that poses the threat. Then, the company should act promptly to engage with the other party, file suit or respond to the complaint or contact law enforcement. Time is of the essence in these situations, but so is clear thinking about potential outcomes, how they may affect the business, and what the company should be trying to achieve when it responds to the trade secret threat. Companies should attend to both.

CD: What advice would you offer to companies on implementing effective processes to protect their trade secrets, and improving their chances of success in any future litigation that may arise?

Homrig: One of the most challenging aspects of effective trade secret protection is balancing risk management with company culture. In litigation, companies must prove that they take 'reasonable measures' to protect their trade secrets, which leaves some room to tailor procedures to reflect company culture. One basic step that all companies should implement is consistent implementation of onboarding and offboarding procedures. Communication is also key. Employees should know the rules, should know what is secret and what is not, such as customer metrics and pricing are secret, but customer lists are not, and should feel comfortable coming forward if they learn of a problem. And companies should document these rules, expectations and communications in an organised way so that they are readily available for litigation.

Epstein: Companies should always implement processes that restrict access to trade secrets on a need to know basis. This can include physical protections such as storing documents and prototypes in locked or restricted areas, technical

protections such as encryption, password protection or other authentication mechanisms to prevent unauthorised access, and even legal protections such as non-disclosure agreements. Companies also should not overlook employee education. It is important for companies to characterise what constitutes a trade secret within the organisation and to educate employees about their responsibilities in maintaining confidentiality. Companies should train employees on the importance of trade secrets, their legal obligations and the company's protection policies in order to foster a culture of awareness and compliance.

de Vrey: It is crucial for companies to take legally correct measures to protect their trade secrets. From an evidential point of view, it is crucial to properly document what the trade secret includes. When describing and protecting trade secrets, companies must be aware of the requirements of the Trade Secret Act. Companies should ensure that their policies and processes are compliant with the law when preparing for potential litigation. By taking such measures it is easier to prove in court that a trade secret exists. Too many companies are not aware of the Trade Secret Act, which may help them protect their trade secrets. The law is a tool, but it is left to the parties to make use of this tool. 'Trade secrecy by design', similar to privacy law's 'privacy by design', means that companies would be advised to 'infuse' the need for keeping information confidential in the organisation and daily operations of the company. This can be done by organising ongoing training, providing practical and user-friendly guidance, and making all personnel aware of the importance of confidentiality.

Pak: The single most important piece of advice I can offer is to follow through once a policy for confidential information is established. In other words, it is important for the company to take steps to ensure that the policy is consistently enforced at all levels and departments. Companies that do not maintain a consistent approach often learn only later, in the course of litigation, that certain employees or departments did not adequately protect certain trade secrets of the company. This is often detrimental to the company's case because the company must demonstrate in court that it took steps to protect its trade secrets from improper disclosure.

CD: Looking ahead, what factors are likely to drive trade secrets litigation? How do you see the landscape developing in the coming years?

Epstein: One of the biggest factors to drive future trade secret litigation likely will be the increasing value of trade secrets with technological

advancements. Trade secret information is becoming increasingly valuable as companies rely on proprietary technology, algorithms and other confidential information to gain a competitive edge. As the value of this trade secret information increases, so does the likelihood that there will be disputes and litigation over its protection. Furthermore, as jurisdictions in the US move away from employee mobility restrictions such as non-compete agreements, trade secret litigation is likely to play an increasingly important role in ensuring fair competition and safeguarding competitive advantages when employees move between competitors. Finally, the landscape of trade secret litigation is becoming increasingly globalised and will likely become even more so in the years ahead. As technology advances and it becomes even easier for companies to touch all corners of the world with their business, trade secret information may become compromised such that plaintiffs will be forced to evaluate different forums for their trade secret misappropriation claims. This introduces additional complexities in both the protection and litigation of trade secrets.

de Vrey: The role of trade secrets will only become more important in the future. Innovation is one of the core principles of doing business in a globalised world and trade secrets are essential for innovation. Companies that do not innovate will not survive. New technologies will provide new challenges. The use of artificial intelligence (AI), with tools such as ChatGPT, may hamper the proper protection of trade secrets. An employee of a company might decide to use ChatGPT to quickly summarise the minutes of a confidential meeting, increasing the risk that the secret information is disclosed. Quantum computing might lead to encrypted trade secrets being accessed by unauthorised persons. In the future, trade secret litigation is likely to be focused on online information. Therefore, the factor most likely to drive trade secrets litigation will be the appearance of new technologies. Most companies will progress protecting their trade secret via encryption. There is a possibility that the rise and increasing value of trade secrets will give way to more aggressive litigation. We can assume that the evolution of new types of technology will greatly enhance new claims. But claims will also be stimulated by bad technical protection of trade secrets.

Pak: Trade secret litigation will continue to be a key tool in the enforcement of IP rights. Employees will continue to move from one company to another, and in certain cases will take with them confidential information that they should not have taken. This will likely only increase in frequency in the coming years. Companies are constantly having to manage their ever-growing, complex network of computers, email

systems, networks and databases, and ensuring that confidential information is secure becomes more and more onerous. In addition, it is also often difficult, impractical or even impossible to protect data, algorithms or source code through copyright or patent law alone. Trade secret law and trade secret litigation therefore continues to be an important avenue for the protection of confidential information for that reason as well.

Homrig: Trade secrets have long been considered a 'defensive' form of intellectual property and parties have traditionally asserted them that way. Whereas companies have often used patent litigation to achieve business goals, such as knocking a competitor out of the market or creating a royalty stream from another company's sales of non-competing products, most companies have historically asserted trade secrets only to protect the actual loss of important information when that loss is likely to cause significant harm to the company. That is beginning to change. With employee mobility so high, 'opportunities' for trade secret enforcement abound, and companies are beginning to use them to achieve business objectives. For example, when a former employee takes trade secrets from Company A to Company B, it may not pose a material risk to Company A – the information may be a trade secret, but not business-critical; the disclosure may be limited; Company B may not be in the best position to use it. But that misappropriation may provide Company A with the opportunity to bring a lawsuit that will make Company B open to acquisition at a lower price, hinder Company B's research and development by diverting resources to litigation, or sow uncertainty among Company B's customers and potential customers. Today, Company A is more likely to bring that lawsuit to achieve those business objectives, where it would not have brought a lawsuit in the past. Because this strategy is so often successful, and because the size of significant monetary judgments is on the rise, this trend will continue. Companies should assess trade secret risk and opportunity accordingly. CD