REPRINT

CD corporate disputes

TRADE SECRET LITIGATION

REPRINTED FROM:
CORPORATE DISPUTES MAGAZINE
OCT-DEC 2021 ISSUE

www.corporatedisputesmagazine.com

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

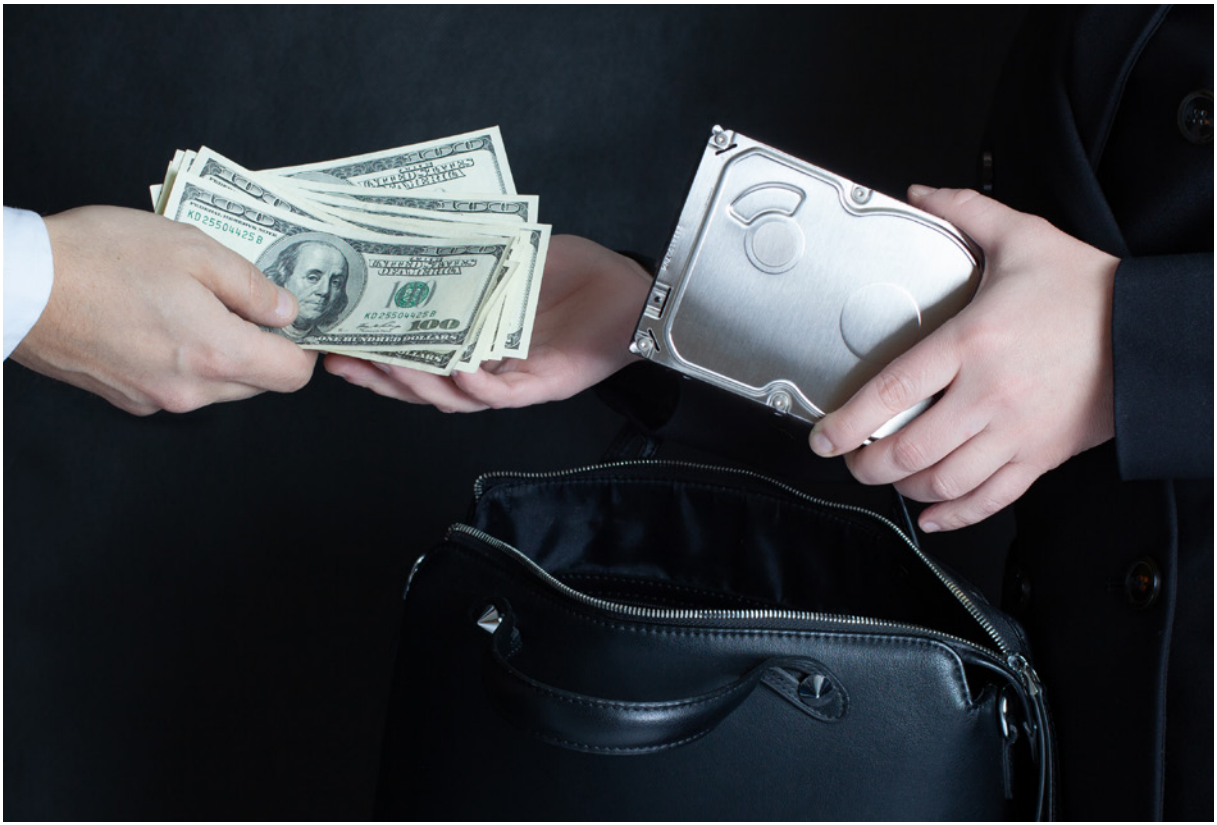
DLA PIPER

Published by Financier Worldwide Ltd
corporatedisputes@financierworldwide.com

www.corporatedisputesmagazine.com

MINI-ROUNDTABLE

TRADE SECRET LITIGATION



PANEL EXPERTS

Paul Steadman
Partner
DLA Piper
T: +1 (312) 368 2135
E: paul.steadman@us.dlapiper.com

Paul Steadman, an experienced first-chair trial lawyer, represents global companies in complex patent, trade secret and other IP-related litigation. He is experienced in ITC and trade secret matters for some of the largest technology and automotive companies in the world. Chambers USA has repeatedly recognised Mr Steadman's practice as "professional, capable and thorough" and says clients are "impressed with the service of the team" and "appreciate the oversight they give". The Legal 500 United States described him as "an outstanding IP litigator" and identified him as one of the "key names" for "trade secret matters, nationally and internationally".

Rajiv Dharnidharka
Partner
DLA Piper
T: +1 (650) 833 2322
E: rajiv.dharnidharka@us.dlapiper.com

Rajiv Dharnidharka handles business disputes and potential disputes, focusing on intellectual property, technology and general corporate matters through counselling, negotiation, litigation, arbitration and mediation. He is the co-chair for litigation of DLA Piper's technology sector group and a member of the FinTech sector group. His main areas of practice are trade secret and software copyright litigation, and he regularly speaks and writes regarding technology issues domestically and internationally. He has been recognised as a leading trade secrets practitioner by The Legal 500 United States and his practice has been recognised by Chambers USA.

Matt Hiller
Partner
DLA Piper
T: +1 (312) 368 2198
E: matt.hiller@us.dlapiper.com

Matt Hiller is an experienced investigator and trial lawyer who represents clients in white-collar, cyber and corporate investigations and complex litigation. A former federal prosecutor, he has led significant and sophisticated criminal and national security investigations and litigation and consulted for state and federal law enforcement and other governmental agencies across the US and abroad regarding cyber investigative techniques.

Leon Medzhibovsky
Partner
DLA Piper
T: +1 (212) 335 4630
E: leon.medzhibovsky@us.dlapiper.com

Leon Medzhibovsky is a highly regarded litigator focusing on intellectual property, trade secret, software and technology-related commercial disputes. He has extensive experience with complex domestic and multijurisdictional commercial technology disputes, as well as high-stakes transactions involving intellectual property assets and cutting-edge technologies. He is a board observer and member of the strategy steering committee for several technology, data/machine learning and software companies.

CD: What do you consider to be among the key trends shaping trade secret litigation in recent months? Have there been any significant legal and regulatory developments in this space?

Steadman: One of the key trade secret litigation trends is the increasing use, and leverage, of trade secret cases at the International Trade Commission (ITC). The ITC has long had the authority and jurisdiction under Section 337 to litigate trade secret cases involving imports to the US, but parties are now using that jurisdiction regularly. And it is quite powerful. If it finds imported goods made using a misappropriated trade secret, the ITC can exercise jurisdiction to issue an exclusion order, keeping imports from entering the US market. This is so even if the trade secret was allegedly misappropriated overseas, and even if the trade secret is used entirely overseas. The ITC can also exercise jurisdiction even if the domestic industry the ITC is protecting does not use the trade secret at all.

CD: In today's digital age, how easy is it for employees, former employees, cyber criminals or other bad actors to misappropriate trade secrets? How would you characterise this risk for companies?

Hiller: The civil and criminal exfiltration of trade secret information has proliferated with the rise in electronic communication, storage and recording applications, and remote work capabilities. Security measures and compliance programmes mitigate risk, but victims often overestimate their security and underestimate their risk from insiders, cyber criminals and even nation states. Each company has a unique risk profile. To better understand that profile, identify vulnerabilities, and have an executable plan in the event of a theft, companies should conduct privileged risk assessments coupled with scenario-based testing. Testing allows a company to plan and practice its response to an exfiltration, including coordinating across business units, information security and technology, in-house and outside counsel, while at the same time preparing for litigation and reporting to law

> **"One of the key trade secret litigation trends is the increasing use, and leverage, of trade secret cases at the International Trade Commission (ITC)."**
>
> *Paul Steadman, DLA Piper*

enforcement. Testing is immensely valuable, because it provides companies with an opportunity to understand their security's capabilities, identify gaps and prepare for a worst-case scenario in a privileged environment.

CD: To what extent have the effects of the coronavirus (COVID-19) pandemic, such as the mass shift to remote working, exacerbated the challenge for companies in safeguarding their trade secrets?

Dharnidharka: The effect of COVID-19 and remote working has been significant, as evidenced by the sharp rise in trade secret actions filed and the countless number of internal issues faced, which largely do not reach the court dockets. As workforces shifted to remote work during the pandemic, many companies' trade secret information was subject to relaxed protective measures, inadvertent disclosures or misappropriation. Employees, business partners and vendors often accessed information using unsecure personal devices, uploaded information to less secure cloud storage systems, perhaps unintentionally, and printed sensitive documents on home printers. As shuttered offices reopen, companies need to develop a process to understand how employees, business partners and vendors stored, transmitted and otherwise used, or misused, trade secret information while working remotely, and then act to identify issues and resolve any problems they have identified. We recommend a five-step process. First, employers need to understand how their employees used company information while working remotely, which can be done with a survey and confirmation process followed by corrective measures as needed. Second, employers should ensure that information is returned, deleted or destroyed, which can and should include forensic analysis of data storage devices for particularly sensitive information. Third, employers should reinstate relaxed or suspended policies and security protocols. Fourth, companies should confirm that their business partners and vendors are protecting the companies' trade secrets following a similar process. Some contracts include provisions requiring

> **"Whether innocently or not, a company's trade secret may end up in the wrong hands and cause significant damage to the company if corrective measures are not swiftly taken."**
>
> *Rajiv Dharnidharka, DLA Piper*

parties to enact and disclose measures used to protect trade secret information. If your contract has such a provision, now is great time to invoke it. Finally, be particularly vigilant with employees, business partners and vendors with whom the company separated during the pandemic. The pandemic and associated business realities forced many companies to lay off employees, including engineers and others with access to important trade secret information. Similarly, economic factors caused companies to end supply relationships, suspend new product lines, exit or shut down joint ventures, and cancel contracts. Whether justified or not, these actions can leave hurt feelings and worse. In such circumstances, whether innocently or not, a company's trade secret may end up in the wrong hands and cause significant damage to the company if corrective measures are not swiftly taken.

CD: When trade secret misappropriation or theft is suspected, what initial steps should a company take in immediate response?

Dharnidharka: The first step is often to retain an e-discovery vendor to forensically image and strategically analyse all potentially relevant data storage devices, including cloud-based accounts, servers and individual devices. The benefit of today's digital world is that nearly every trade secret case can be largely supported by the data trail. The trick is often finding the data and accurately assessing it. Conducting an early and accurate approach to forensic analysis can both set the case on the right track and avoid pitfalls based on false assumptions.

Medzhibovsky: It is important to clearly define the trade secrets. Unlike other areas of intellectual property, such as patents, copyrights and trademarks, trade secrets are not registered or prosecuted with any governing body. Accordingly, your trade secret identification is not predetermined years in advance. Define your trade secrets broadly enough to protect the technology but narrowly enough so that you can establish confidentiality and independent economic value. Also keep in mind that you can identify multiple trade secrets and compilations comprising trade secrets.

Hiller: The circumstances of the theft – internal versus external – will dictate the scope of the response and the victim's initial priorities. In general, however, victims of potential criminal theft should consider the following. First, protect privilege. Second, preserve potentially relevant digital information that could assist the investigation – from email to phone logs to door swipes to logins to digital audit trails. Third, identify the perpetrator's digital internal and external footprint, such as personal email, social media and IP addresses used to login from home and personal devices. Fourth, identify why the information qualifies as a trade

secret and the steps used to keep it a secret, which is essential to assisting law enforcement obtain warrants and being able to explain it in common sense fashion. Fifth, identify key witnesses and documents. Finally, contact law enforcement as soon as possible. When criminal and civil remedies are pursued together, victims and their counsel also should consider any ethical obligations, including whether they could be using criminal allegations to obtain an advantage in a civil matter or engaging in extortion.

CD: If the matter progresses to litigation, what factors are needed to prove the company's trade secrets qualify for protection and that their misappropriation caused substantial operational, financial and reputational damage?

Medzhibovsky: The general standard to show that a trade secret qualifies for protection is relatively low: something that is reasonably maintained as confidential and has independent economic value because it has been maintained as confidential. As to the second element, there is no quantum requirement; any independent economic value can suffice. But this low standard should not give a plaintiff comfort. If the trade secret does not have substantial economic value, the time, cost and uncertainty of litigation may not be warranted.

Dharnidharka: With regard to causation of damages, the best evidence is loss of a sale to a competitor in one-on-one competition where the competitor used the plaintiff's trade secret to obtain the sale. Without this one-to-one evidence, the most persuasive evidence often comes in the form of the plaintiff's reliance on the trade secret to maintain and advance its business – and how the trade secret is the differentiating factor. Finding similar evidence in the defendant's discovery can have the same effect. Finding credible third-party evidence of the same, including industry publications, can also be persuasive.

Steadman: In the ITC, there is no requirement to prove damages, but one element of the case is harm to a domestic industry. So, in addition to proving the existence of a domestic industry, the complainant is going to have to show that the misappropriation of trade secrets and importation of products is harming the domestic industry. This is a somewhat different standard than many parties are used to in patent cases at the ITC and needs to be studied carefully and understood.

CD: How crucial is the involvement of expert witnesses in trade secret cases? In what ways can they assist?

Medzhibovsky: For technical trade secret cases, technical experts are a must-have. A well-versed

expert with industry experience and an ability to clearly and persuasively articulate the state of the art at the relevant time, the advancement in the art achieved by the trade secret, and the value it bestows on the owner, and the defendant, can help a plaintiff achieve its burden of proof. The plaintiff should assess whether an industry expert will be more persuasive than a gifted professor who has never worked in the field or vice-versa. Many times, both are needed, especially in a jury trial where different perspectives resonate differently with different jurors. If both a professor and an industry participant are necessary, which is not unusual, retain two experts – one for each perspective. It is very rare that one expert fully covers both perspectives and a shortcoming in one area can impact the otherwise persuasive nature of the testimony in the other area. For non-technical trade secrets, whether an expert is necessary or even worth the cost can be a closer call. It is important to interview and try to retain experts early in a litigation because having the right experts will shape fact development and overall litigation strategy.

Steadman: In defending a trade secrets allegation, the experts are just as critical. The defending party is going to want to show that the claimed trade secret is really just industry knowledge, or that it was never taken or used. If there is liability, the defending party is going to want to assign a low value to the secret, and to show that it can be designed around in order to avoid a crippling injunction. And at the ITC, each party will need a third expert, an economic expert who can quantify the domestic industry and the harm to the domestic industry with evidence and argument that is persuasive to the Commission and its administrative law judge. Many of the economic experts who appear at the ITC have been doing so for a very long time, over a large number of cases, and already know the legal and economic tests that the Commission is looking for. If you use someone new, make sure that you carefully review the applicable tests, and meet them.

> **"If the trade secret does not have substantial economic value, the time, cost and uncertainty of litigation may not be warranted."**
>
> *Leon Medzhibovsky, DLA Piper*

CD: What essential advice would you offer to companies on managing, conducting and winning trade secret cases?

Dharnidharka: Organisation and preparation are key. Be ready to clearly define your trade secrets and have an elevator pitch ready to deliver to the judge, and the clerks, so that your trade secrets are readily understood. This is key to obtaining discovery and framing your case. Be able to articulate the metes and bounds of your trade secrets – especially if they are technical in nature – how they are maintained as confidential and exactly how they derive independent value from being maintained as confidential. Jettison the useless. Know as much as you can about how your adversary has used and benefitted from using your trade secret and how you have been damaged. Retain technical and damages experts early, especially if your trade secret relates to a new technology without a well-established market.

Steadman: A surprisingly large number of these cases, in the ITC and in court, turn on discovery. The party that fails to preserve or produce the evidence can be sanctioned by the presiding judge in ways that will irreparably harm the remainder of the case. It is absolutely critical to muster and preserve the applicable evidence at the front end of the case, whether or not you represent the trade secret owner or the alleged misappropriator. But it is equally important to convince the client to produce the evidence – even harmful evidence. Many foreign defendants are not used to US discovery rules and want to withhold things like emails or documents. But this inevitably comes out in discovery and can result in severe sanctions.

> **"A crisis is not the time for owners to understand their capabilities, limitations and gaps. Time will be of the essence, and preparedness can be the difference between mitigation, recovery and loss."**
>
> *Matt Hiller, DLA Piper*

Hiller: To have the best opportunity to prevent, recover and mitigate trade secret theft by bad actors, trade secret owners should consider the following. First, understand the capabilities and limitations of your security and processes. Second, have a plan and a team, including outside counsel, ready to respond to a potential theft. Third, be able

to articulate the basis for trade secret treatment of the information and how it is protected plainly and concisely. Finally, know how to get in touch with law enforcement which is capable of responding to such a theft in an emergency. A crisis is not the time for owners to understand their capabilities, limitations and gaps. Time will be of the essence, and preparedness can be the difference between mitigation, recovery and loss. CD