Bloomberg Law®

May 29, 2025

Non-Disclosure Agreements Shield Buyers and Sellers in M&A Deals

David Kappos
Cravath

Kathryn-Ann Stamm
Cravath

Vincent Joralemon
Cravath

Cravath attorneys explain how robust NDAs help protect trade secrets and reputations during and after the mergers and acquisitions process.

The Bottom Line

- Properly crafted non-disclosure agreements protect both buyers and sellers in all types of strategic transactions, including mergers and acquisitions, when they clearly define the rights and obligations of both parties.
- NDAs must be explicit about what information is confidential, how long it must be kept secret, and what the receiving party is allowed to do with the information it receives.
- Misappropriation can be found even when a receiving party's product doesn't directly incorporate a trade secret—prevent this with a careful scoping of authorized uses under the NDA and assess whether other projects touch on the subject.

Imagine sharing your company's most valuable information in pursuit of a lucrative strategic transaction only to find that, after discussions fall through, that same information is used against you in the marketplace.

This scenario could have become a costly reality for Zest Labs after the startup shared details of its produce-tracking system during potential partnership talks—only to see the other side build out their own produce tracking system shortly after such talks fell through. Fortunately for Zest Labs, a confidential information non-disclosure agreement was in place, resulting in a $222 million verdict from an Arkansas federal jury for willful misappropriation of trade secrets.

Just as NDAs can protect disclosers such as Zest Labs, they are equally critical for recipients. Imagine being on the other side of the table—receiving sensitive information, negotiating limited rights to it and ultimately walking away from a failed deal—only to face claims of misuse. Without proper protections in place, such disclosures can become a liability for the discloser or the recipient of confidential information.

However, for those with well-crafted confidentiality agreements, remedies for such misappropriation are available. This highlights a fundamental lesson: non-disclosure agreements aren't mere formalities, but essential tools for protecting confidential information—provided they are carefully drafted.

NDAs have long served as essential safeguards for confidential information shared in the context of merger and acquisition discussions, collaborations, and other high-stakes business dealings.

Recent court decisions remind us that the precise drafting and enforcement of NDAs can mean the difference between safeguarding your confidential information and facing devastating financial and competitive loss if you are the discloser, or facing the prospect of a debilitating injunction or damages award if you are the recipient.

Protecting against these risks requires a strong understanding of the key rights and remedies that NDAs provide—and how courts enforce them.

Rights and Remedies

At their core, NDAs are legally binding contracts that regulate the use and disclosure of non-public, confidential, or proprietary information. NDAs foster trust by enabling candid negotiations and establishing clear rules for handling exchanged materials, while providing recourse in case of a breach.

NDAs are designed both to deter the receiving party from misusing or disclosing confidential information and, if such misuse occurs, to provide a mechanism for the disclosing party to obtain remedies that compensate any resulting harm, including the diminished value of the compromised information.

A recent example of monetary remedies occurred in *CardiAQ Valve Technologies v. Neovasc, Inc.*, in which the court found Neovasc misappropriated CardiAQ's trade secrets to develop a competing device. Because Neovasc had signed an NDA explicitly restricting its use of proprietary data shared by CardiAQ, CardiAQ secured a $91 million judgment.

Recognizing that monetary damages alone may be insufficient to compensate fully the harm tied to a breach of an NDA, they often explicitly provide for injunctive relief to preserve the inherent value of the compromised information.

For example, in *SiOnyx LLC v. Hamamatsu Photonics K.K.*, the court issued an injunction transferring Hamamatsu's patents to SiOnyx because the parties' NDA stipulated that SiOnyx, the disclosing party, received ownership of the information and patent rights stemming from their agreement.

Similarly, in *Syntel Sterling Best Shores Mauritius Ltd. v. TriZetto Group Inc.*, TriZetto successfully blocked Syntel's parallel work using source code, manuals, and guides covered under the parties' NDA in their service agreement.

Although injunctions provide important recourse for breach, such remedies can be highly disruptive, preventing activities otherwise permissible but for the NDA.

The threat of such injunctive relief may enhance the effectiveness of the NDA as a deterrent to misuse of shared confidential information. The scope of the NDA, both in terms of captured confidential information and its permitted uses, should be specifically tailored to the needs of the transaction at hand to avoid undue burden on the contracting parties.

Beyond enforcement mechanisms, NDAs must also be carefully structured to define the rights and obligations of both disclosing and receiving parties.

Rights and Responsibilities

Well-drafted NDAs should not only address liability and remedies for breach, but also require the receiving party to ensure that adequate safeguards are in place on the part of anyone with whom it shares the information—whether affiliates, employees, or other "representatives" as defined in the agreement.

For example, in *Ajaxo Inc. v. E*Trade Financial Corp.*, E*Trade was found liable for misappropriating trade secrets and breaching an NDA related to Ajaxo's wireless stock trading technology. The court found that, although E*Trade didn't directly develop a system incorporating the applicable trade secrets, it shared Ajaxo's confidential information with Everypath Inc., which then developed a similar system.

Because this secondary misappropriation violated the NDA, the court held E*Trade liable for the actions of its representatives and awarded Ajaxo $1.3 million in damages. The key takeaway: NDAs that explicitly account for misuse beyond the direct parties—including by third parties that receive and exploit confidential information—provide critical protections for disclosing parties.

A carefully drafted NDA doesn't only protect the interests of disclosing parties. It can also shield the receiving party from disputes by clearly defining permissible uses of confidential information.

In *Wal-Mart Stores, Inc. v. Cuker Interactive, LLC*, Walmart contracted with Cuker to update a website for its UK subsidiary. Critically, the court found that the agreement failed to specify any intended use beyond the work order. When Walmart later applied some of the updates to its US-based website, Cuker sued, claiming Walmart exceeded the scope of its license.

Finding that Walmart hadn't explicitly negotiated the right to use the updates on its US website, the court granted Cuker a multimillion-dollar trade secret misappropriation judgment and a permanent injunction prohibiting Walmart from using any code, files, or programmatic references developed by Cuker in Walmart's US activities.

The core lesson: Contracting parties must carefully outline what a receiving party can—and can't—do with protected information. Failing to do so can be just as harmful to the receiving party as it is to the disclosing party.

Clear Parameters

NDA enforceability hinges on how precisely the agreement sets forth core provisions, including confidentiality parameters, the duration of protection, and the permitted uses of confidential information.

A common point of contention is the scope of what must be treated as "confidential" under the agreement. Disclosing parties typically favor broad confidentiality definitions that cover all non-public information, while recipients push for a narrower scope to facilitate legitimate use and reduce exposure to unclear liabilities.

Subtle differences in how information to be treated as confidential is defined can have significant legal ramifications.

Consider *Olaplex, Inc. v. L'Oréal USA, Inc.*, in which the court rejected Olaplex's claim that L'Oréal misappropriated trade secrets because Olaplex failed to specify confidential information under the agreement with sufficient "specificity" and beyond "a high level of generality."

In contrast, in *SiOnyx v. Hamamatsu*, the parties agreed to an NDA with a provision granting SiOnyx ownership of the information and all patent rights "in or arising from" the information shared pursuant to the parties' agreement to evaluate applications and joint development opportunities using SiOnyx's black silicon photonic devices.

After the agreement ended, Hamamatsu developed a "black silicon" photodiode, referring to prototype work completed with SiOnyx. Finding that such use was covered under the expansive terms of the NDA, the court granted SiOnyx ownership of all US and foreign patents arising from the technology covered under the agreement.

Parties also should anticipate how they may need to use confidential information they receive. They should carefully define the NDA's "purpose" regarding the use of confidential information and assess whether other projects might involve that information or touch on its subject area. Misappropriation can be found even when a receiving party's product doesn't directly incorporate a trade secret.

For example, in *AMS Sensors USA Inc. v. Renesas Electronics America Inc.*, AMS successfully alleged that Renesas misappropriated its trade secrets by using proprietary data to redesign its products and develop a new line of light sensors—even though the sensors didn't directly incorporate AMS's proprietary technology. The $48 million judgment against Renesas underscores that even indirect use of confidential information can result in substantial liability.

Clearly drafted NDAs can protect receiving parties after failed negotiations. For example, in *Olaplex v. L'Oréal*, Olaplex shared particular trade secrets in acquisition talks with L'Oréal, and L'Oréal used those secrets in its "build vs. buy" analysis (that is, whether it was more cost-effective to acquire Olaplex or launch its own product). When talks collapsed, Olaplex claimed that L'Oréal had misappropriated those trade secrets and used them to build its own model.

However, the court sided with L'Oréal, noting that, under the NDA, Olaplex "explicitly gave L'Oréal authorization to use the information in that way." To preempt such disputes, NDAs often require the return or destruction of all shared confidential information upon request or upon termination of the NDA, with limited exceptions for legal or regulatory compliance.

The clearer these terms, the less likely disputes will escalate into costly litigation when deals fall through.

Conclusion

The lessons from the case law are clear: An NDA is only as strong as its drafting, enforceability, and the foresight of the parties involved. To mitigate risks, companies should ensure that NDAs precisely define the scope of protected information along with any restrictions or permissions on its use.

Parties should carefully consider what information they share or are willing to receive, and whether it's truly necessary for the intended purpose of the NDA. As courts scrutinize not just the definition but also the use of confidential information, businesses must take a proactive approach in crafting agreements that withstand legal challenges.

Ultimately, a well-structured NDA serves as a vital tool for protecting the business interests of both disclosers and recipients of confidential information in a highly competitive marketplace.

This article does not necessarily reflect the opinion of Bloomberg Industry Group, Inc., the publisher of Bloomberg Law and Bloomberg Tax, or its owners.

Author Information

David Kappos is a partner at Cravath and co-chair of the firm's intellectual property practice.

Kathryn-Ann Stamm is of counsel at Cravath, advising clients about their intellectual property and technology assets.

Vincent Joralemon is an associate at Cravath.

Cravath, Swaine & Moore LLP