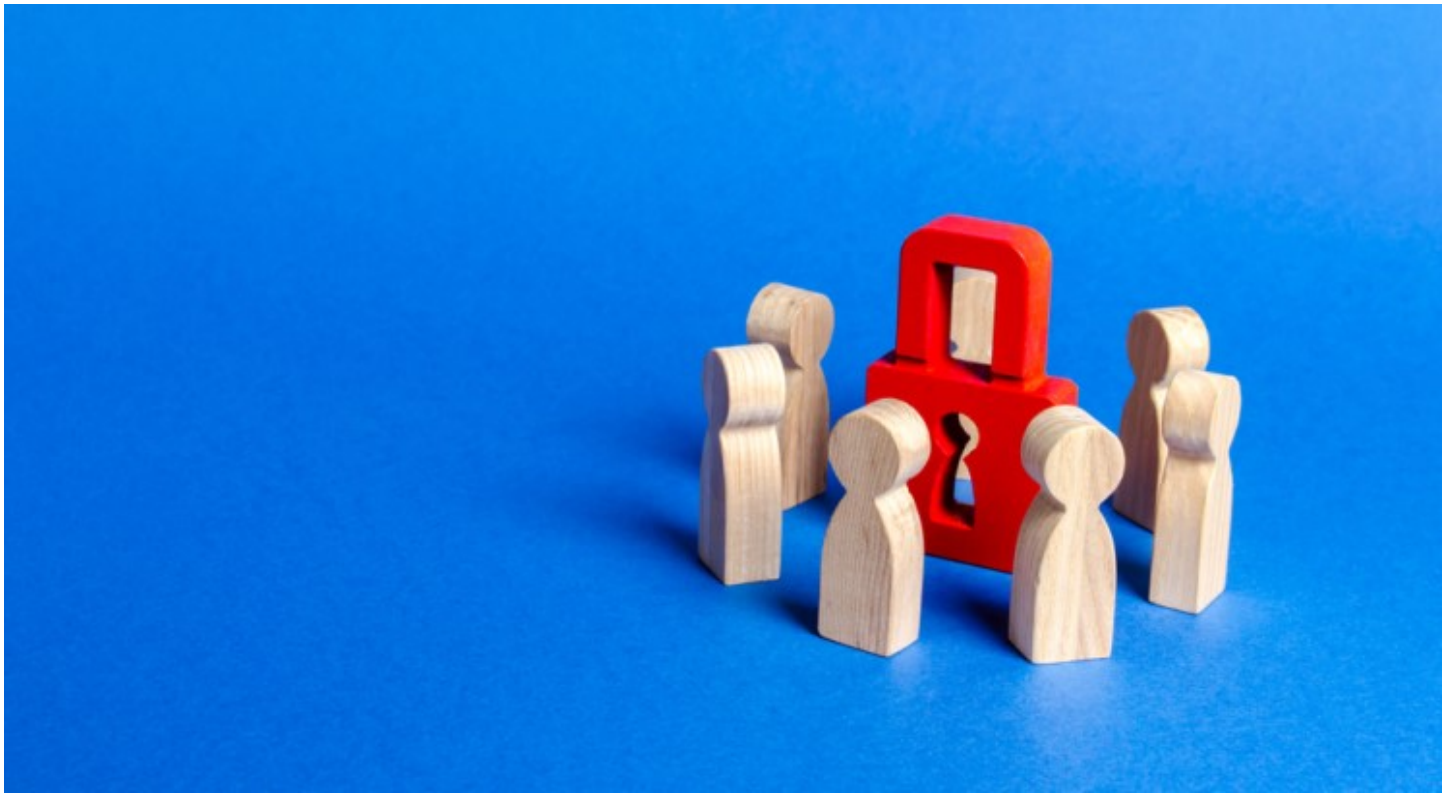
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

Best Practices to Protect Trade Secrets in Failed Acquisitions and Customer Relationships

Intellectual Property

Litigation and Dispute Resolution





In part one of this three-part series on best practices for protecting trade secrets and guarding against claims of trade secret misappropriation, we examined some practice pointers for protecting trade secrets when key employees move from one competitor to another. In this second part, we

discuss some best practices for protecting trade secrets and guarding against allegations of trade secret misappropriation in failed corporate acquisitions or customer-supplier relationships.

In many technology fields, discussions around potential acquisitions and due diligence frequently occur. Although acquisitions can have many potential benefits, veterans of the start-up and emerging company sectors know that, more often than that, negotiations and due diligence exercises fail to lead to an actual corporate merger or acquisition.

Thus, a target company should take practical steps to prevent the unnecessary dissemination of its trade secrets, and the potential acquirer should also take steps to prevent the unnecessary sharing of a target company's trade secrets, even potentially with their own technology development team.

Staging due diligence

First, a potential acquirer should try to structure its discussions and due diligence to prevent being imbued with every potential target company's trade secrets. At the outset, a potential acquirer may be looking at several potential targets.

In this first round, a potential acquirer may only need to review confidential financial information and business plans to determine if there is interest. In that case, the acquirer should enter into a commercials-only NDA with the target company. Should both sides wish to continue discussions, then in a second round, the parties could enter into a separate NDA that allows for the disclosure of technical trade secret information.

Contractual clauses to consider in an NDA

If the potential acquirer is independently developing technology in the same space as the target company, consider postponing receipt of any technical, confidential information from a target company until the independently developed technology is publicly released.

However, if the acquirer cannot wait that long, document in the NDA that the potential acquirer is already innovating in that same space, and nothing in the NDA would prevent the acquirer from continuing to innovate in that space, provided they don't use the target company's trade secrets. Such a clause can be very useful at trial to refuse the argument that the acquirer could only develop the technology in question through theft.

The potential acquirer may wish to ask for a residuals clause in the NDA. The basic concept of a residuals clause is that any ideas, concepts, facts, or details that remain purely in a person's mind is a "residual" and use of the "residual" is not actionable. This is a potentially powerful clause to protect against trade secret misappropriation allegations down the road because any knowledge that resides in a person's mind after engaging in due diligence would not be deemed trade secret misappropriation.

From a target company's perspective, agreeing to such a clause could demonstrate to the acquirer that your trade secrets are more substantial than "de minimis" details, and that the target company is confident that no person could truly remember how to re-create those trade secrets simply by recalling what he saw during due diligence. However, there certainly remains some risk for a target company that a residuals clause eliminates the ability to later assert that a potential acquirer misappropriated some specific know-how from the target company.

A standard clause found in commercial NDAs is a “need to know” clause. A best practice, although burdensome, is to document, prior to receipt of any trade secret information, who at the acquiring company is receiving the information, why they “need to know,” and that those individuals agree to abide by the terms of the NDA. Getting the target company to acknowledge and agree that these “need to know” individuals can see the trade secrets also forms a good level of protection.

Acquirers should also ensure that any NDA has a firm expiration date, complete with a description of what obligations expire. As an acquirer, you don’t want to find yourself at trial arguing that the confidentiality obligations must have expired by a specific time if there is not a clear expiration clause spelling out what duties expire.

Target companies will want to ensure that the NDA specifically carves out trade secrets from the expiration clause and specify that the obligations regarding the protection of trade secrets last as long as the trade secrets still meet the statutory definition under the applicable state statutes.

Some courts have found that a trade secret holder fails to exercise reasonable care in maintaining the secrecy of its trade secrets if the NDA imposes confidentiality obligations on trade secrets only for a limited duration. On the other hand, NDAs should not impose confidentiality obligations in perpetuity as such clauses run the risk of being deemed an unreasonable restraint on trade.

Finally, NDAs should have a “destroy on demand” clause. Target companies will want the recipients to certify that they have destroyed all copies of confidential information from their systems, and such certifications should be signed and provided in a documentary form. Acquirers, as recipient companies, should ask for a “reasonable efforts” provision so that if one electronic document happened to persist in some remote repository and gets discovered later, it does not constitute a breach of the NDA.

Acquirers should, as a best practice, designate a person or small group of people at the outset as the people responsible for destroying all copies of confidential information received should a deal fall through. Develop a checklist that aids this person in searching for and identifying all the places where confidential information from a target company might reside so that they can be checked and wiped.

Due diligence best practices

Nowadays, a virtual document clean room is a mandatory best practice. Such virtual clean rooms prevent any user from downloading or copying any sensitive documents. The clean rooms limit access to only authorized individuals who ideally have been disclosed and approved by the parties prior to gaining access.

A virtual clean room also provides a log of activity, showing exactly when a document was accessed and for how long. Once the deal is complete, or the parties have decided not to pursue a deal any further, all the information in the virtual document clean room can be deleted, or at a minimum, the recipients’ access can be revoked.

If there is no virtual document clean room, acquirers must impose rules that documents received from target companies cannot be forwarded to others in the company and that those documents must not be stored on company shared drives or cloud storage. The danger associated with inadvertent syncing of a cloud storage accounts with people’s mobile devices is too high to permit employees to store a target company’s trade secret information in a cloud account.

If possible, separate the team reviewing a target company's trade secrets from the product development team that is independently developing a competing technology. If such a clean separation is not possible, then a "residuals" clause in the NDA is that much more important.

Concluding a deal

If the acquirer decides not to pursue a business relationship after reviewing the trade secrets, contemporaneously document the reasons for the decision and reasons for going in a different direction. If the acquirer detects flaws or problems in the technology, document them. These documents can be internal — what's important is that they be contemporaneous.

If there is a successful acquisition, ask the new onboarding employees for their prior employment agreements. The acquiring company should decide whether the new incoming employees need to sign new employment agreements, certifying that they are not using any third-party trade secrets to develop the technology.

Most importantly, a company needs to maintain consistent practices and procedures across all of its employees; otherwise, any exceptions or aberrations will be seized upon by litigants in a trial and highlighted as negligence or malfeasance.

Conclusion

The variety of best practices all impose different costs, loss of speed, and burden to the due diligence process in an acquisition discussion or a potential customer-supplier relationship. However, choosing a few of these best practices and balancing them against the need for speed by the business teams in a company will go a long way to protecting against theft of trade secrets or allegations of trade secret misappropriation.

Walton Norfleet



IP Counsel

Smiths Group plc

He handles a wide variety of IP-related matters and has broad experience in the industrial, energy, medical, and software fields.

Eugene Y. Mar



Leader, Technology industry group

Farella Braun + Martel

He specializes in trade secrets, patent, and IP licensing litigation and advises both Fortune 100 and emerging companies on best practices for trade secret protection.