Bloomberg BNA

WORLD INTELLECTUAL PROPERTY REPORT >>>

News and analysis on IP law, regulation and policy from around the world. For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 31, NUMBER 3 >>> MARCH 2017

Patents/Trade Secrets

Managing Confidential Info in M&A and Commercial Transactions

Ed Black and Nicole Cabrera

By Ed Black (partner) and Nicole Cabrera (associate), Ropes & Gray LLP, Boston; email: Ed.Black@ropesgray.com, Nicole.Cabrera@ropesgray.com

There are many complexities to managing disclosures and protecting intellectual property assets while negotiating mergers, acquisitions and commercial transactions. Trade secret misuse looms heavily in practitioners' minds. Exchanging confidential and even privileged information can be critical to getting the deal done. Yet there is a risk that one party may steal the other party's information if the deal doesn't close, or that both parties may waive privileges or rights against third parties.

Practitioners have several tools at their disposal to minimize these risks. To manage the risks arising in a broken deal, a properly drafted non-disclosure agreement is key, along with best practices in information distribution and tracking. To manage the risk that privileges may be blown, proper establishment of 'common interest' or 'joint' communication privileges should be added to the list. These practices, which are particularly useful in a U.S. setting, are discussed below.

Non-Disclosure Agreements (NDAs).

NDAs should be in place from the outset of negotiations. The general purpose of these NDAs is well established. Prior to disclosing any confidential information, parties should execute an NDA prohibiting one or both parties from using the disclosed information for any purpose other than evaluating, negotiating and consummating the transaction without the disclosing party's consent, and requiring each party to use commercially reasonable methods to keep disclosures confidential.

Buyers and sellers may also agree to carve out extremely sensitive confidential information and address it separately under a special NDA.

Within this framework, however, there are specific adjustments that may favor recipients or buyers versus providers or sellers. These inflection points are where a buyer or seller can attempt to gain a greater level of protection, although often it is a zero sum calculation with more protection for one party reducing protection for others.

Categorical or designated definitions of confidential information: How confidential information is defined can expand, favoring information providers with expanded protection, or narrow, which would favor information recipients by narrowing protection and expanding freedom to operate. Narrower terms tie the definition to written notices, written labels and other express acts of designation. Broader terms eliminate formal designation requirements and tie the definition to categories, including the expansive categories of 'anything a reasonable person would regard' as confidential information, or 'anything disclosed' at a specific time, place, or within a certain time frame.

Exclusions: NDAs routinely supplement the definition of confidential information with a separate list of express exclusions that can dramatically narrow or expand protection favoring one side.

Common exclusions operate to exclude from the definition information that (i) the buyer already knows; (ii) the buyer independently develops; (iii) the buyer is legally required to disclose; (iv) is publicly known or accessible, or in the public domain, and (v) is disclosed to the buyer by a third party who does not owe a duty of confidentiality to the seller.

While exclusions of this type are standard, buyer and seller favorable variations exist. Seller-favorable variations establish a 'burden of proof' test requiring that, for an exclusion to apply, the party claiming exclusion must demonstrate its applicability through written records or sworn certifications. Buyer-favorable variations can dial back the burden of proof by applying exclusions based on recipients' 'reasonable belief' that the exclusion applies.

Residual knowledge clauses: Residual knowledge clauses directly address the use of information from a broken deal that is held in a party representative's unaided memory. Broad or buyer-favorable versions simply recite that the parties are free to use and exploit 'residual knowledge in unaided memory.' Indeed, the buyer-favorable versions may have a supporting stipulation or non-assert covenant where the seller agrees, and promises not to contest, that the parties are in similar industries and may be properly engaged in similar projects. Hence there will be no presumption of misappropriation arising from mere similarity.

Where residual knowledge clauses are combined with this waiver of presumptions, the buyer has strong protections against the most common seller complaint: that after the deal failed, the would-be buyer put a similar product on the market and must have misappropriated.

In contrast, a seller-favorable residual knowledge clause often uses the 'burden of proof' approach to limit residual knowledge use and establish presumptions from similarity. Here the NDA provides that use of residual knowledge is permitted, but only when supplemented by documentary evidence of related independent development. In an agreement where such evidence is expressly required, there is an implication that the parties intend that the lack of such evidence suggests misappropriation supporting the presumption that may arise from similarity.

Return and destruction: Most NDAs provide some arrangement for the potential buyer to return, destroy, or otherwise stop using provided confidential information if the deal fails. Again, there are numerous inflection points that can push this clause in favor of one party or the other, including: whether (i) the 'return or destroy' duty is automatic or must be requested, (ii) evidence of certification of destruction must be provided, (iii) the duty extends to metadata and automatically created archival and backup copies, and (iv) the duty extends to all representatives of a party (such as attorneys and accountants.).

Agreement term: NDAs commonly endure for so long as deal discussions are ongoing and some period thereafter. In a buyer-favorable form, the period is a fixed and short term, often one year. In a seller-favorable form, the term may be for as long as the provided information retains its confidential status, or a longer period of years, often three to five years, and in rare cases even longer.

Communication Controls.

Buyers and sellers can work together to manage the risk of misappropriation liability by controlling the method and review of their disclosures. Online data rooms offer a variety of services that help parties employ many of the following communication control techniques. Once again, there are inflection points where these tools can be managed to favor the seller/provider or the buyer/recipient:

Scope of audience: The degree to which access to materials is broadly or narrowly allowed can have a significant effect on the risk of alleged misappropriation.

Systems allowing narrow access often favor the recipient

   ISSN 0952-7613

by providing evidence that information did not get into the wrong hands. Broad distribution can favor the information provider, as proof of access is a key element of most claims for misappropriation or infringement and broad access can support that element. Of course, managing to actually protect secrets may be of more practical importance than managing to win litigation, in which case narrow disclosure may work for both parties.

Staging disclosures: Parties should stage disclosures, with the most strategically valuable confidential information being disclosed at or near closing. Since a buyer's decision to close may hinge on its review of the seller's most strategically valuable confidential information, the buyer may insist on accessing all such confidential information prior to signing. Rather than comply, the seller may prefer to walk.

Mark documents: The disclosing party should mark all disclosures as "Confidential." Sellers typically resist marking because accidental failure to do so can lead to unprotected confidential information. Online data rooms, however, make it relatively easy for sellers to uniformly mark their disclosures.

Protecting Against Third Parties.

Traditionally, parties to a commercial transaction have relied on the common-interest doctrine to preserve attorney-client privilege of information disclosed between the parties after signing but prior to closing. The argument is that the privilege applies because the parties share a common interest in the transaction and have a common adversity to third parties who may be suing or threatening to sue the seller or deal target.

In *Ambac Assurance Corp. v. Countrywide Home Loans Inc.*, 27 N.Y.3d 616(2016), the New York Court of Appeals narrowly interpreted the common-interest doctrine, holding that a communication must relate to legal advice in pending or reasonably anticipated litigation against both parties for the privilege to survive. This suggests that a shared commercial interest that has not yet perfected through deal closing is not sufficient to establish the necessary common interest. In doing so, the court fomented a great deal of uncertainty as to the best practices for managing privilege in commercial transactions where the litigation requirement is unlikely to be satisfied.

We do not have a 'silver bullet' cure for the Ambac problem, and the commercial necessities of a transaction may require that certain information be disclosed prior to closing, risking a privilege waiver. We believe, though, that this risk can be mitigated through the following best practices (i) to establish the strongest argument for the presence of the common interest privilege under the circumstances, and (ii) to control communications so that if a privilege is waived, the damage is minimized. We discuss each of these approaches in turn below.

Common Interest Privilege.

The common interest privilege varies in its articulation across jurisdictions in the U.S. Outside of the U.S., the privilege often doesn't exist at all. In the U.S., the most common versions of the privilege have many of the following elements:

Privileged communication: Only privileged attorney-client communications are eligible for protection under the common interest doctrine. Attorney-client privilege protects confidential communications between privileged persons (e.g., client & attorney) for the purpose of obtaining or providing legal assistance to the client.

Common legal interest: Jurisdictions vary in their definition of "common legal interest." Some require that parties share an "identical" legal interest (e.g., New York) while others merely require a "sufficiently similar interest" (e.g., Massachusetts). If the parties enter into a common interest agreement, they should explicitly state their shared legal interest and should persuasively present the degree of similarity between their interests.

Some jurisdictions only extend the privilege to communications disclosed at a time when the parties have a common legal interest, meaning that communications disclosed before the development or after the end of a common legal interest may not be protected. To increase the odds of preserving attorney-client privilege, parties should wait to make sensitive communications until a time when the parties have a common legal interest.

Litigation requirement: Depending on the jurisdiction, the common interest privilege may be limited to disclosures relating to litigation. Where this requirement exists, the common interest privilege is unlikely to apply if parties do not share litigation-related common legal interests.

Some jurisdictions require that the disclosure relate to pending or reasonably anticipated litigation (e.g., New York), while others require pending litigation (e.g., Texas), and still others have no litigation requirement whatsoever (e.g., Massachusetts, Delaware, California, as well as the Second, Third, Seventh and Federal Circuits). If possible, parties should state that each of their communications is made in connection with pending or reasonably anticipated litigation.

Legal advice: Some jurisdictions require that the communication contain legal advice to qualify.

In jurisdictions that require that communications concern legal advice (e.g., Delaware), communications concerning litigation will satisfy this requirement. Communications concerning business transactions may also satisfy this requirement, provided they involve regulatory, compliance or other legal matters.

By contrast, communications that only deal with business interests will not. If possible, parties should include some legal advice in their communications to bolster their claim that they are privileged.

Confidential communication: Communications must be kept confidential to stay within the common interest doctrine. Disclosing information to third parties who do not share a common legal interest with the disclosing party can waive the privilege.

Best practices for maintaining the confidentiality of communications include disclosure tracking, marking documents "Confidential and Privileged" and limiting the number of people who have access to the materials.

Written agreement: Although many jurisdictions do not have a formal writing requirement for invoking the common interest doctrine, a written agreement can serve as a contemporaneous record of the parties' shared legal interest and can rebut the suggestion that the parties cooperated for merely commercial rather than legal reasons.

Parties should execute a common interest agreement prior to making any disclosures. The agreement should identify the shared legal interest and, if applicable, the pending or reasonably anticipated litigation. If possible, the agreement should be governed by the law of a jurisdiction that recognizes a broad common interest privilege. Parties should consider marking each communication as made pursuant to the agreement.

Communication by counsel: The common interest doctrine is intended to protect disclosures between attorneys in order to facilitate the coordination of legal strategies. Communications between separately represented clients, outside the presence of their respective lawyers, may not qualify for the common interest privilege. To the extent possible, attorneys should share information with one another rather than with the parties directly.

Communication Strategies.

In-house counsels have a number of tools at their disposal to render communications made during deal talks less helpful to future third party litigants. Though these practical steps do not establish a legal privilege, they make it less likely that sensitive information will be discovered by future third party litigants and, if such information is discovered, make it less useful to adversaries.

Oral communications: If parties suspect that their communications will not be privileged under the common interest doctrine, they might consider orally disclosing strategically valuable confidential information. Before a seller does this, it should ensure that the NDA's definition of confidential information includes oral disclosures.

Qualified communications: When possible, parties should qualify their written communications. For example, one way for a seller to do this is to present to the buyer a hypothetical fact pattern and a conclusion based on it. The seller does not state whether the hypothetical fact pattern is analogous to its real-world situation. Rather, the buyer has the burden to investigate whether the hypothetical fact pattern accurately reflects the seller's situation and thereby judge the value of the seller's conclusion.

In response to a fact pattern and conclusion posed by the buyer, the seller can confirm the buyer's conclusion based on the proposed facts but refuse to confirm whether the buyer's fact pattern accurately reflects the seller's real-world situation.

Alternatively, a seller can express its opinion or conclusion to a question posed by a buyer, subject to an ongoing need to investigate further. In other words, the seller may express its current conclusion with the caveat that its conclusion may evolve over time or in response to new information or developments.

Communication by counsel: If the parties believe they may be sued by a third party in the future, they can try to limit the pool of possible deponents and witnesses that the third party can call. One way to do this is to have the parties' counsel communicate with one another rather than with the parties themselves.

Metadata risks: Before sharing any materials, parties should clear all metadata from their communications. Some examples of metadata that may be stored in a document include the name of the document's author, names of previous authors, document revisions, document versions and more. Rather than risk exposing this metadata to future third party litigants, parties to a transaction should remember to clear metadata before sharing it with one another.

Ultimately, parties' disclosures and communications should be managed in response to business needs and goals. To the extent, however, that practitioners can employ the foregoing tips and practices without compromising the business-side's strategic vision, the risks attendant to sharing sensitive information will be reduced.

The authors are part of Ropes & Gray's intellectual property transactions practice.

ISSN 0952-7613