Risk Transfer: Indemnification for Damages Arising Out of Data Breaches and Cyber Incidents

Jean M. Lawler
Lawler ADR Services, LLC
Los Angeles, California

Most commercial disputes involving business to business issues will arise out of, or at least involve, a contract. That contract generally will be for services to be rendered and/or for products to be provided. Commercial contracts will usually include an indemnity provision whereby one party agrees to indemnify the other for a loss or damage that the other party has caused.

1. Contractual Indemnity

Using California law for purposes of discussion, California Civil Code § 2772 defines indemnity as “a contract by which one engages to save another from a legal consequence of the conduct of one of the parties, or of some other person.” "Generally, indemnity is defined as an obligation of one party to pay or satisfy the loss or damage incurred by another party*." Rideau v. Steward Title of California, Inc.* (2015) 235 Cal.App.4th 1286, 1294*.*

Whether direct damages are recoverable by the indemnitee pursuant to the indemnification clause or via direct claims for breach of contract, negligence, and the like, turns on the language of the indemnity agreement.

"A contractual indemnity provision may be drafted either to cover claims between the contracting parties themselves, or to cover claims asserted by third parties." *Ibid.* Whether an indemnity agreement covers direct liability, third party liability, or both, is a question of contract interpretation. *Rossmoor Sanitation, Inc. v. Pylon, Inc*. (1975) 13 Cal.3d 622, 633.

This distinction between indemnity for direct and third-party liability can be important in a data breach/cyber situation. As explained in *Zalkind v. Ceradyne, Inc.*, (2011) 194 Cal.App.4th 1010, 1024-1025:

> Although indemnity generally relates to third party claims, "this general rule does not apply if the parties to a contract use the term `indemnity' to include direct liability as well as third party liability." ( *Dream Theater, Inc. v. Dream Theater* (2004) 124 Cal.App.4th 547, 555 [ 21 Cal.Rptr.3d 322].) "[E]ach indemnity agreement is `interpreted according to the language and contents of the contract as well as the intention of the parties as indicated by the contract. `"(*Wilshire-Doheny, supra*, 83 Cal.App.4th at p. 1396.) When indemnity is expressly provided by contract, the extent of the duty to indemnify must be determined from the contract itself. (*Rossmoor,*

> *supra*, 13 Cal.3d at p. 628; see also *Heppler v. J.M. Peters Co.* (1999) 73 Cal.App.4th 1265, 1277 [87 Cal.Rptr.2d 497] ["parties to an indemnity contract have great freedom of action in allocating risk, subject to certain limitations of public policy"]; *Rooz v. Kimmel* (1997) 55 Cal.App.4th 573, 583 [64 Cal.Rptr.2d 177] ["We must determine the scope of a contractual duty of indemnification . . . from the contract itself."]; *Myers, supra*, 13 Cal.App.4th at pp. 968-969 ["The extent of the duty to indemnify is determined from the contract."].)
>
> "[T]he question whether an indemnity agreement covers a given case turns primarily on contractual interpretation, and it is the intent of the parties as expressed in the agreement that should control. When the parties knowingly bargain for the protection at issue, the protection should be afforded. This requires an inquiry into the circumstances of the damage or injury and the language of the contract; of necessity, each case will turn on its own facts." (*Rossmoor, supra*, 13 Cal.3d at p. 633.) The indemnity provisions of a contract are to be construed under the same rules for interpreting contracts, "`with a view to determining the actual intent of the parties. `"(*Wilshire-Doheny, supra*, 83 Cal.App.4th at p. 1396; see also *Maryland Casualty Co. v. Bailey Sons, Inc., supra*, 35 Cal.App.4th at p. 864.)

In the cyber arena, indemnification for both direct liability and third-party liability can come into play in numerous ways, usually vis-à-vis vendor relationships.

Examples can include situations when there has been a cyber incident where a Managed Service Provider is perhaps hosting and managing a business' computer network. It can involve an IT vendor who provides onsite services to maintain a business' network. Networks might "go down" and not be operable. There may be an attack on a network that disables it. There might be an actual data breach of ransomware attack. All these situations were caused by something, i.e. who let the bad guys (also known as "threat actors" in? Software might not be patched, or not patched properly. Portals may have been left exposed. Passwords might not have been protected. Proper protocols may not have been in place on the system. Maybe more than just the computer system was accessed – maybe the threat actors exfiltrated personally private information of clients, customers, patients, students, consumers in general. Whether on the dark web or not, the fact that such information is "out there" in the nether world creates its own set of liability issues. The causation questions can be endless.

But one thing will be clear, if there is any potential liability exposure on the part of the vendor, the business will seek to recover damages from the vendor for whatever money it spends to get its own systems back up and running and to protect its system from further harm, to respond to people whose information was stolen and/or to pay settlements to injured third parties, and to otherwise pay to make the injured party "whole". Damages may also include regulatory fines and

penalties, attorney fees, expert costs, notification costs and compensation for loss of customer goodwill.

That said, the vendor in turn may turn to its own vendors, asserting that the vendor's vendor is the legally responsible party, in turn triggering its own right to recover damages from that vendor.

For sake of this discussion, the terms "indemnitor" and "indemnitee" are key terms. The indemnitor in the above example is the vendor who has the contractual duty to indemnify the damaged business, the damaged business being the indemnitee. The rights and obligations of each will be set forth in the terms and conditions of the indemnification clause in the contract. The specific terms of each indemnification clause will vary based on the individual agreement, each contract being unique to itself, the parties and the circumstances for which indemnity is to be provided.

The most expansive type of indemnification agreement will be one where the indemnitor assumes all liability of the indemnitee, *including the indemnitee's own, active or sole, negligence, where allowed by law*. This is not the type of indemnity agreement that will generally be found in vendor contracts in the cyber space. More typically, if the indemnitor assumes all liabilities, it will only be for those liabilities where the indemnitee was not actively or solely negligent. The indemnification language with the least obligations being assumed by the indemnitor, which is also typical in the cyber space, will be one which indemnifies only for the liabilities created by the indemnitor, not those caused by anyone else.

How any given indemnity provision applies to a particular circumstance requires analysis of the contract terms as they relate to the facts of the loss. Ultimately, if the parties do not agree on who owes what to whom and the dispute cannot be resolved without resorting to litigation or arbitration, contract interpretation being a matter of law will mean that the Judge or Arbitrator will decide the issue.

2. Insurance Coverage for Contractual Indemnification Obligations

Commercial contracts typically also call for certain types of insurance to be maintained by one party or the other, and usually calls for the indemnitee to be named as an additional insured on one or more of the indemnitor's insurance policies. At the very least, the parties will want the indemnitee named as an additional insured on whatever third-party liability policy of the indemnitor would be applicable to a cyber loss. That said, there are multiple ways that insurance coverage can come into play regarding data breach and cyber-related damages.

First and foremost, the indemnitee may have its own insurance policy that provides it with coverage for a particular loss. First party coverages would apply to the direct damages incurred by the indemnitee while third-party coverages

would provide the indemnitee with defense and indemnity against the claims of third parties. That said, if the indemnitee's own insurer pays these damages and expenses for its insured, and if there is an indemnity provision that applies to the loss, then the insurer would most likely subrogate to the rights of its insured against the indemnitor, seeking reimbursement for the money it has paid out for which the insured would have been entitled to indemnification from the indemnitor.

Secondly, the indemnitee may be an additional insured under a policy of insurance issued to the indemnitor that provides coverage for it for a third-party loss. If that is the case, then the indemnitor will tender its defense to that insurer (either instead of its own or in addition to its own), requesting that the indemnitor's insurer defend and indemnify it against third party claims as an additional insured. If the indemnitor's insurer agrees to defend and indemnify the indemnitee against that third-party loss, then that will generally satisfy the indemnity obligation of the indemnitor to the extent of that aspect of the loss. In other words, the indemnitor has insured itself against the indemnity risk that it assumed in favor of the indemnitee. In this circumstance, whatever the indemnitor's insurer pays out for defense of the additional insured indemnitee will not reduce the available liability limits of the indemnitor's policy, leaving more money available to pay for losses.

If the indemnitor's insurer does not agree to defend and indemnify the indemnitee as an additional insured, the indemnitee will have a breach of contract claim against that insurer and would still have its indemnification claim against the indemnitor. It may also have a breach of contract claim vs. the indemnitor for not having procured insurance that it was contractually obligated to procure. The indemnitee's direct insurer may have contribution and//or equitable indemnification claims against the additional insured insurer for what it pays out on behalf of its own insured.

Thirdly, even if the indemnitor's insurer picks up the defense and indemnity of the indemnitee as an additional insured, the indemnitee's direct claims vs. the indemnitor for damages that it suffered (as opposed to third-party claims) would be for the indemnitor's insurer to pay as damages on behalf of the indemnitor. Presumably a vendor in this field will have a Cyber Insurance policy or some other type of policy providing it with coverage for such liabilities.

Finally, the parties should make sure that the indemnitee receives an actual additional insured endorsement from the indemnitor's insurer, to confirm its additional insured status. A certificate of insurance is not an additional insured endorsement and should not be deemed to convey additional insured status to the certificate holder even if there is a notation to that effect typed into a box near the bottom of the form. Read the first sentences at the top of the Certificate of Insurance and be warned. Get an actual additional insured endorsement.

While this is certainly important to the indemnitee, it is equally important to the indemnitor who wants to make sure that it has appropriately transferred its risk to the insurer to defend and indemnify the indemnitee against a third-party claim. If relying only on a Certificate of Insurance, it may be that the indemnitee's tender of defense will be denied and the indemnitor will be left owing that indemnification obligation none-the-less. If there is no additional insured status for the indemnitee, then not only could the indemnitor be sued for breach of contract for failure to procure insurance as required by the contract, but any damages incurred by the indemnitee for which the indemnitor's liability policy makes payment, will be treated as damage payments, reducing the indemnitor's available liability limits for future claims.

3. Conclusions and Closing Comments

Drafting contractual indemnity clauses that will provide for the intent of the parties is critical at the outset, and may be the most important part of the contracting process. In addition to indemnity provisions, hold-harmless and insurance requirement provisions are usually included in commercial contracts. The clauses should be clear and concise, without ambiguity. The contractual obligations, under both the contract with the indemnitor and under applicable insurance policies, need to be clearly understood by all who are in a position to have an impact on the viability of recovery under the indemnification provision or insurance policies.

When there is eventually a loss, to protect the indemnitee's rights under the contract with the indemnitor and under all applicable insurance policies, the following things should be done:

a. analysis should be given first to the indemnity, hold-harmless and insurance requirement clauses to determine if the loss falls within the scope of the indemnity to be provided and additional insured insurance may be applicable to protect the indemnitee for the loss;

b. a tender and demand to indemnify (to also defend if a third-party suit) should be made to the indemnitor at the earliest opportunity;

c. all insurance policies of the indemnitee should be reviewed and analyzed and notice provided to any insurer under whose policy there may be coverage for the loss; and

d. a tender and demand to defend and indemnify should be made to the additional insured insurer (the indemnitor's insurance under which the indemnitee is named as an additional insured) and a request should be made for a copy of the policy if necessary

When there is eventually a loss, to protect the indemnitor's rights under the contract with the indemnitee and under all applicable insurance policies, the following things should be done:

a. The indemnitor and its attorneys should also review the indemnity, hold-harmless and insurance requirement clauses of the contract with the indemnitee;

b. If an indemnitor's vendor is involved, that contract and those insurance policies should be reviewed and notices provided in accord with the suggestions above for an indemnitee; and

c. Notice should be given to all insurers whose policies of insurance may be applicable.

There are of course a myriad of other things that need to be done to respond to the cyber incident or data breach itself, but to the extent of indemnification and insurance, this action list is a good start.

Dealing with indemnity provisions and insurance policies can get complicated, but understanding the interplay between indemnity agreements and applicable insurance policies is very important.