LIABILITY LIMITS

BREAK THE LOGJAM – HAVE A BUSINESS DISCUSSION

Few topics generate more heat (or less light) than abstract debates about liability limits, horrific 'worst cases' and allegedly 'standard' terms. Suppliers, customers and their advisors care deeply about these things – as they should, given the risks. Occasional headlines about security incidents remind decision-makers of potential 'worst cases.'

How, then, to get past this and reach an acceptable, negotiated resolution? Actual and perceived risks vary according to circumstances. So do companies' tolerance for risk and preferred negotiating positions. Counsel may suggest helpful approaches and structures but there are no silver bullets.

One technique has proven remarkably effective: business conversation about underlying realities, risks and potential solutions. Few business decision-makers have committed to memory finer points of law about consequential damages; but they well understand the risks to their business.

On the suppliers' side, counsel and sales teams must be prepared to articulate the reasons for their positions:

- No prudent, sophisticated supplier will 'bet the company' on any single transaction. Liability for occasional errors or malfunctions must be limited. Unlimited liability must be limited to a few, egregious situations, such as intentional wrongdoing or gross (ie, extreme) negligence.
- Suppliers do not write insurance. If they did, policies would have limits and prices would rise to offset risk premiums for risks that may or may not be insurable at acceptable cost.
- Suppliers' solutions help to reduce, but cannot eliminate all risk, any more than fire alarms and sprinklers can eliminate all risk of fire.
- Suppliers are accountable (within limits) when they are at fault, but not for circumstances outside their control, including their customers' acts, omissions and decisions. Liability must be limited proportionally to the extent of the supplier's fault.
- Usual liability limits on major engagements provide ample protection and assure the customer of the supplier's engagement and attention should things go wrong.
- Basic limitations on liability should generally be sufficient to make the customer whole by covering costs of corrective work and, in dire situations, substitution of another supplier or solution; but suppliers cannot insure customers against all secondary effects (ie, consequential damages) or such business losses as reductions in profit or share prices.

CONTINUED

COMMENTARY | LIABILITY LIMITS

This publication is a summary of legal principles. Nothing in this document constitutes legal advice, which can only be obtained as a result of a personal consultation with an attorney. The information published here is believed accurate at the time of publication, but is subject to change and does not purport to be a complete statement of all relevant issues.

Before wading into proposed language, suppliers' negotiating teams should discuss with customers their concerns in depth and in business terms. The most serious questions almost invariably concern security and the risks associated with security incidents.

- What most concerns the customer? Keeps decision-makers awake at night?
- Where does the company do business, and in what industry? Special requirements apply in some regulated industries (eg, health care, banking). Laws vary around the world, but often impose essentially similar obligations in somewhat **different ways. Everywhere, privacy, security and data protection laws are becoming more stringent.**
- What kinds of data are at risk? Ordinary business information? Personal data? Health, financial or other sensitive data? Risks differ. So may regulatory requirements (eg, HIPAA for hospitals and clinics, PCI for retailers and others who deal directly with consumers).
- How well are the data protected today? What works well or needs improvement? Are there clear standards for classes of data and particular systems and operations? What plans exist for addressing known weaknesses and emerging risks?
- What does the customer believe it needs and, equally important, what is it willing to invest and to pay? Few commercial enterprises need, or can afford, the kind of fail-safe security that suppliers may offer to law enforcement, the military or intelligence agencies. Not every commercial customer needs the levels of protection that regulators require for banks, stockbrokers or hospitals.

From discussion of these realities, consensus may emerge first upon actual (rather than theoretical) risks and a technical and operational solution that will satisfy the customer's needs at acceptable cost. Then, and only then, can the parties wade into the fine print. Debates about abstractions are rarely productive.

Liability limits are often the last issue to be resolved, and negotiated resolutions vary for a variety of reasons, including the transaction's scale and risks, but the usual framework remains much as it has been for many years: (i) exclusion of consequential or indirect damages and such business losses as lost profits; (ii) a ceiling upon damages for all manner of claims; often with (iii) an enlarged ceiling for an range of information security and privacy claims; and (iv) a short, heavily negotiated list of exceptions for which liability is unlimited, including intentional wrongdoing, gross negligence, some (though not necessarily all) indemnified claims and the customer's payment obligations. Within this framework, many variations are possible, but the ultimate decisions on both sides about sufficiency of remedies and the supplier's risk tolerance are business decisions – decisions that should be informed by candid business conversations about risks, solutions and costs.