

“Tricks” of the Trade: (Un)limited Liability for Information Security

Article By:

Doneld G. Shelkey

Valerie A. Gross

In some circles, lawyers have a bad reputation for being tricky little buggers who use tools like precision wording and careful drafting to “lawyer up” simple tried-and-true business concepts, such as “the parties will work together to . . .” Whether or not trickery is ever intended, it is always very important to pay attention to not only what concepts appear in an agreement but also where concepts appear.

Limitations of liability are big-ticket review items for all types of transactions. In most sectors, a limitation on damage types (e.g., consequential damages) and a limitation on damage amounts (e.g., damage caps) are market provisions. The real battleground, however, is on the exclusions to such limitations. For many service providers, no matter the starting position, the first round of revisions will typically include customary carve-outs for breaches of confidentiality and third-party indemnification claims. Aggressive or ill-tempered negotiators may ask for more, or agree to less, but we find that most lawyers who routinely work in this space will agree to the above two carve-outs, even if they grumble about it a bit.

Keeping the above in mind, it is also important to note that many form agreements, especially those that come from a vendor, do not initially include robust data privacy and security provisions. At most, there may be a reference to a website detailing security terms or an obligation to use “commercially reasonable” protective efforts in the warranty section, but it is also exceedingly common for a vendor to omit the concept entirely. Thus, the onus is on the customer to insert protective information security provisions that are appropriate for the proposed transaction.

The above typical scenario serves as the perfect petri dish for trickery-most-foul (whether or not intentional). We’ll explain.

Where does one insert the information security provisions? Good lawyers tend to hold red ink as a precious resource. Not having to renumber an agreement, with all of the associated cross references, is also a nice bonus. Scanning through the headings for an appropriate place to insert the information security provisions, an economical lawyer will likely look past the “Services” section, the “Change Management” section, and perhaps pause to consider the “Warranty” section until he or she comes

across the “Confidentiality” section. After all, a data breach is fundamentally related to confidentiality. A few minor tweaks to the subsection numbering, and the entire information security section can be dropped into the agreement without so much as glancing at the remainder of the subsection references. Done and done.

The issue, of course as noted above, is that breaches of the confidentiality section are routinely carved out of the limitations of liability without much of a fight. The limitations of liability are prone to begin like this:

Except for breaches of Section 11 (Confidentiality) or claims subject to Section 12 (Indemnification), in no event shall . . .

If so, inserted language would (intentionally or unintentionally) represent an unlimited liability for a data breach. Depending on the sector and the nature of the transaction, the request itself and even the approach may be perfectly reasonable, but we find that clients time and time again will miss this particular import during negotiations. In fact, it has happened enough in our practice that we thought it would be prudent to call it out in a blog post.

Copyright © 2025 by Morgan, Lewis & Bockius LLP. All Rights Reserved.

National Law Review, Volume VI, Number 98

Source URL: <https://natlawreview.com/article/tricks-trade-unlimited-liability-information-security>