

*"The Perfect Fit for  
Your Business"™*

**ROBERT H. CARPENTER, JR.**

ATTORNEY AT LAW  
5912 CASTLEBAR LANE  
PLANO, TEXAS 75093

—  
TELEPHONE 972.473.4834

—  
email: [Bob.Carpenter@CarpenterLaw.net](mailto:Bob.Carpenter@CarpenterLaw.net)

—  
[www.CarpenterLaw.net](http://www.CarpenterLaw.net)

October 2005

---

---

## Damages for Data Security Breaches

Information technology outsourcers and their service providers must engage in a reasoned, rationale discourse on the difficult topic of risk allocation for data security breaches.

### Boilerplate or Hot Plate?

Remember that “boilerplate” language in your information technology outsourcing agreement? No doubt there’s a provision that goes something like this:

Regardless of anything else in this agreement and to the greatest extent permitted by law, no court, tribunal, arbitrator or presiding officer of any administrative or other proceeding may award to Customer any special, indirect, consequential, speculative or incidental damages (including, without limitation, lost profits or goodwill) or punitive damages in any dispute (including, without limitation, any dispute based on alleged fraudulent, willful or dishonest conduct) against Company, and Customer expressly, completely and irrevocably waives any right to obtain such damages in connection with any such proceeding.

And then, this qualitative limitation is probably coupled with a quantitative one something like this:

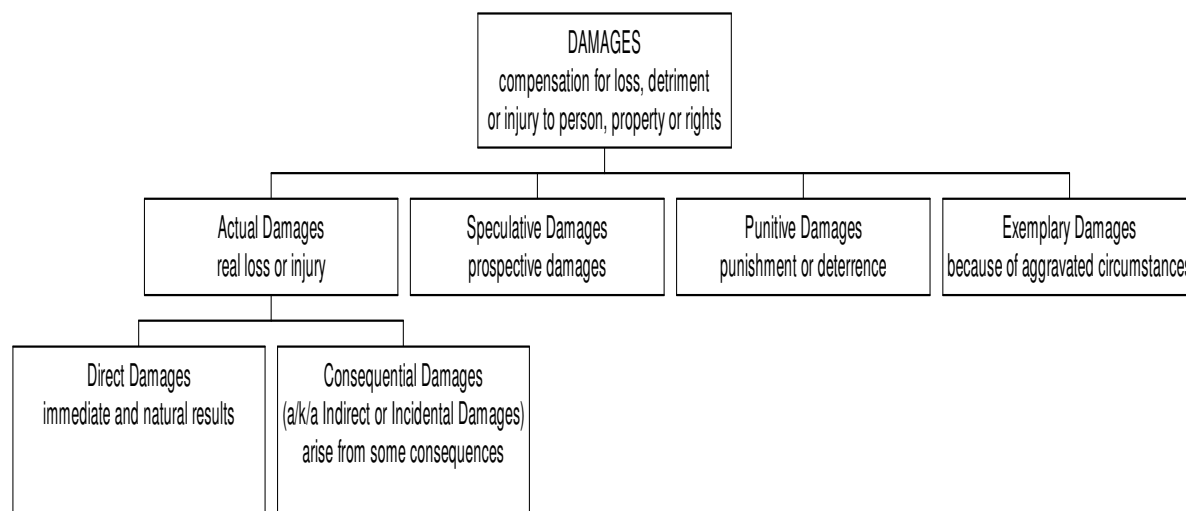
Company’s liability with respect to any claim based on services provided under this agreement is limited to the total fees and charges actually paid to Company for such services in the 12-month period before that occurrence.

### Damages Tree

Damages, like people, come in many shapes and sizes. The best way to illustrate them is by using a “tree” like this one:<sup>1</sup>

---

<sup>1</sup> No doubt, another attorney might reorganize the boxes. Regardless, the importance of visualizing the concept of “damages” is useful to appreciate the nuances of words used in contracts such as “actual damages” and “direct damages.” The differences can be startling and quite unintended by at least one, and maybe both, of the parties.



In the event of a data security breach, direct damages are not likely to be large. But, the consequential damages could be. The loss of customer goodwill and the potential consequences of identity theft from such a breach can reach enormous proportions. Further, the plaintiffs’ class action bar has argued, and no doubt will continue to argue, for punitive damages as a prophylactic to further data compromises.

Of course, speculative damages, while purely conjectural shortly after the occurrence of an event, can ripen into direct damages claims. They are likely to form the basis for class actions and regulatory complaints that will result in settlements that include damages elements that compensate for future possibilities.

### **Risk Limitations**

The qualitative and quantitative risk limitation provisions quoted above are representative of limitations on liability typically included in commercial contracts. Information technology service providers, those who possess, process and transmit the nonpublic data of their customers, have long sought to exclude all but the actual and direct damages caused by their actions and to strictly limit their dollar exposure to allowed damages.

These provisions present a significant potential financial downside to the outsourcing company that has long accepted this risk. Previous client newsletters have observed that such provisions are now among the most often and most hotly negotiated. In today’s environment, the outsourcing company that bears the risk of data security breaches is essentially at the mercy of its vendor.

### **Insurance**

Vendors have almost always secured coverage for their technology errors, including data loss and security breaches. But carriers have been willing to underwrite that coverage with the understanding that the vendor’s agreement has limited damages. Thus, errors and omissions insurance has often been a misleading resolution to the liability question. Now, the insurance market for technology errors and omissions coverage is tightening. Electronic payments processors (*i.e.*, those that process credit and debit card transactions) are finding that carriers have shut the door on their industry because of recent notorious electronic data compromises.

Outsourcing companies can buy their own errors and omissions coverage, but many do not. They cite the high cost. And, they are now demanding that their vendors accept responsibility for data compromises that result from the vendors' actions, at least those of negligence and intentional or criminal conduct. Vendors reply that there must be some risk sharing if they are to continue providing outsourcing services at a competitive rate.

### **“Honest” Negotiations**

The reasoned and rational discussion that is advocated here must transcend the typical outsourcing industry practices. Both parties have good arguments for their perspective.

The public, and regulators, have become more sensitive to the risks of electronic data compromise. In essence, this is a “new” risk. One that has not been fully appreciated before, and one that has not presented the potential for financial loss that it now does.

In that context, outsourcing company and vendor must reevaluate risk allocation. The vendor's responsibility is to create a safe and secure infrastructure and process that will, within commercially

**In addressing urgent data security concerns, “Ouch!” – the July – August 2005 Carpenter Law Client Newsletter – noted:**

Security must be a significant focus for all of those who provide and use data in a technology-driven environment. Both ownership and confidentiality are tightly wound with data use and are the conceptual elements of data security. They are not new topics of interest to those who outsource some, or all, of their technology requirements; but today they are a business issue and a legal concern.

**In December 2004 Carpenter Law observed in “Data Processors, Forced to Reevaluate Pricing Strategies?” that the most negotiated provisions of data processing contracts are**

. . . the quantitative cap on damages and the qualitative prohibition for damages other than actual monetary losses (*i.e.*, incidental, consequential, special or punitive damages).

. . . Allowing for special damages above and beyond actual damages, particularly with regard to data security and privacy, could subject a vendor to business crippling liability.

**These client newsletters are available at <http://www.carpenterlaw.net/newsletters/archive/dnewsletters.html>.**

reasonable standards, protect the data entrusted to it. The customer must decide the value proposition that such precautions present. This value proposition translates into either (a) higher vendor charges for a guarantee of security through more comprehensive insurance and greater assumption of risk or (b) greater assumption of risk by the outsourcing company, which can be hedged by insurance.

Either of these alternatives requires a very careful and thoughtful negotiation and documentation of the information technology outsourcing arrangement and a new boldness from all participants.

**© 2005, 2007 Robert H. Carpenter, Jr.**

This client newsletter is for informational purposes only, and is not intended to be legal advice. Transmission of this newsletter is not intended to create, and its receipt does not establish, an attorney-client relationship. Legal advice of any nature should be sought from legal counsel.

IRS CIRCULAR 230 DISCLOSURE: Notice regarding federal tax matters: Internal Revenue Service Circular 230 requires us to state herein that any federal tax advice set forth in this communication (1) is not intended or written to be used, and cannot be used, for the purpose of avoiding penalties that may be imposed by federal tax laws, and (2) cannot be used in promoting, marketing, or recommending to another person any transaction or matter addressed herein.