



*"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)

July – August 2005

---

---

## Ouch!

Headlines like those to the right should be enough to make everyone – consumers, businesses and technology providers – sit up and take note. And, they are only a few of such headlines during the past 12 months.

**Citi Unit Loses Data on 4 Million**

*Tape Delivery "Lost" En Route*

***Hackers Tap CardSystems Solutions Data***

40 Million Cardholders May Be Affected

**CHOICEPOINT ADMITS DATA COMPROMISED**

**CREDIT DATA ON MILLIONS SOLD TO THIEVES**

And, now, the Federal Government is getting into the act:

**CONGRESS RESPONDS TO  
DATA-SECURITY FEARS**  
Legislation would mandate data security  
programs and consumer notification

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.

### **"Just One" Is Not Enough**

Ownership and confidentiality are opposite sides of the same coin. Each is important to the customer that outsources the processing of data. And, these are intricately bound with the permissible uses for a vendor that processes data.

## *Confidentiality*

Users of outsourced information technology services are all too familiar with the need for confidentiality. The Gramm-Leach-Bliley Act, a recent Congressional mandate to financial institutions, requires confidentiality for the “nonpublic personal information” of a customer.<sup>1</sup> In fact, *all* information that anyone shares with an information technology outsourcer should be treated as “confidential.” But what does that really mean?

Most confidentiality provisions go something like this:

The parties will receive and hold all information communicated to one by the other, whether before or after the date of this agreement, in strict confidence, will use such information only for purposes of this agreement and will not disclose such information without the prior written consent of the other party.

Essentially, the parties to such a provision are promising to keep each other’s information secret and not to disclose it to third parties (and perhaps within their own organization only to those who have a “need to know”), unless the law requires otherwise.<sup>2</sup>

The parties are also promising to limit the use of such shared information to those related to the contractual relationship. In an information technology agreement this limited use concept is critical. Any other use of that data (*e.g.*, sale of such data or its derivatives) places it beyond the effective control of its owner, who is ultimately responsible for its security.

## *Ownership*

In outsourcing the processing of data, the data’s owner must not only ensure the secrecy of the data it supplies to its processor, but also its ownership rights. In an information technology outsourcing contract, the party that is providing the data to the processor should declare its sole ownership. In connection with that declaration, the owner again limits the use of such data by its processor.<sup>3</sup> And, the service provider implements appropriate measures to safeguard the data entrusted to it.

## **Data Security**

For some time now Federal and state bank regulators have expressed concerns over data security in outsourced technology arrangements. Through numerous regulations, they have established for financial institutions a vendor management process the ultimate thrust of which requires that an outsourcing financial institution know the business of its service provider almost as well as the provider itself does. This requirement is accomplished through due diligence

---

<sup>1</sup> See Gramm-Leach-Bliley Act § 501(a), 15 U.S.C. §6801(a) (2000).

<sup>2</sup> Some provisions include additional language that requires each party to treat the other’s information with the same degree of care applicable to its own information. While such a standard may seem desirable, tying one’s duty of care to an industry standard is probably the better alternative.

<sup>3</sup> There are exceptions, most notably in marketing. Some retail merchants sell scanned data from bar-coded merchandise, along with demographic data, to marketing data aggregators that use it to identify buying habits.

focusing on the financial, technical and managerial components of the provider and its service.

This guidance has translated to electronic payments, and the card payments industry leads the way through the card associations' PCISS—the Payment Card Industry Security Standard—and such brand specific programs like VISA's CISP, or Cardholder Information Security Program. While these programs focus primarily on a processor's data security measures, there is a growing trend to, like with financial institutions that outsource, place part of the burden on merchants that accept electronic payments to ensure that service providers have in place appropriate data security measures and that the merchant itself has implemented such measures.

### *Due Diligence*

So, if the end-user of technology services is to have responsibility for an outsourcer's data security, what rights (and obligations) should it have in its contract with the service provider? The vendor management programs of the banking regulators require an investigation of a service provider's financial, managerial and technical resources. These programs also place a continuing burden upon the customer to monitor these factors throughout the outsourcing relationship.

This is a good start for any user of outsourced technology services. And, this due diligence obligation begins when the customer has the most flexibility, the vendor selection process. What, however, should a customer expect after the relationship is formed?

### *Contractual Rights*

After the contract has been signed, both vendor and customer cannot stand still. Data security is an ongoing and mutual responsibility. To set expectations firmly at the inception of the relationship, the contract should include at least some of the basics. First, the parties should agree to comply with all applicable laws. While this may seem obvious (and in reality duplicates an already existing obligation), such a covenant provides an injured party with an immediate contractual remedy.

Second, the service provider should have an obligation to inform the customer of its security policy and practices, and the customer should have the right to terminate the contract if its vendor is not adhering to those previously agreed upon standards. Of course, there are limits to the data security details that a vendor should provide because too much information could compromise the very goal of the data security program. On the other hand, the customer is not looking for the "how" so much as the "what."

This kind of information can be communicated in very broad objectives and measured by periodic reporting. In fact, objective reporting for such programs is available through SAS 70<sup>4</sup>

---

<sup>4</sup> The SAS 70 audit, or service auditor's report, employs internationally recognized auditing standards developed by the American Institute of Certified Public Accountants (AICPA) and demonstrates whether a service organization has implemented appropriately designed control objectives and control activities that are operating effectively. *See* AM. INST. OF CERTIFIED PUB. ACCOUNTANTS, REPORTS ON THE PROCESSING OF TRANSACTIONS BY SERVICE ORGANIZATIONS – SAS NO. 70, available at

audits, security program certifications and internal audit reports. Executive summaries of these types of reports should be a requirement of the vendor's contract. In cases where different or more detailed information is needed by a customer, that customer might contract for the right to compel the vendor, at the customer's expense, to engage a mutually agreeable third-party to perform testing and issue two levels of reports—one at the executive summary level to inform the customer about its specified control objectives, and another at the detail level so that the vendor may identify failed objectives or weaknesses through thorough testing, which would support the ineffectiveness of the objectives, and have recommendations for remediation. Such a mechanism satisfies the customer's needs without compromising system data security.

### A New Kind of SLA

The service level agreement, or SLA, is now a well-recognized means of measuring performance quality. Perhaps this concept should now be applied to data security.

There are, no doubt, established standards for data security. Those set forth in the payment card industry's PCISS are an excellent example. Other standards may be found in recent legislative mandates like California's Assembly Bill 1950, which became effective in mid-2003:

Any [business] that maintains computerized data that includes personal information [e.g., social security number, driver's license number, and bank or card account number] that the [business] does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.<sup>5</sup>

When negotiating an information technology contract, carefully consider data security. Ensure that confidentiality and data ownership, as well as uses, are appropriately covered. Provide qualitative and quantitative metrics for measuring compliance with the data security requirements that the contract includes.

© 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.

[http://www.cpa2biz.com/AST/Main/CPA2BIZ\\_Primary/AuditAttest/Standards/SASs/PRDOVR~PC-060441PDF/PC-060441PDF.jsp](http://www.cpa2biz.com/AST/Main/CPA2BIZ_Primary/AuditAttest/Standards/SASs/PRDOVR~PC-060441PDF/PC-060441PDF.jsp) (last visited Sep. 26, 2007).

<sup>5</sup> CAL. CIV. CODE § 1798.29(b) (West 2006) available at <http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29>.

### OTHER CLIENT NEWSLETTERS

May 2005's client newsletter "C<sup>3</sup>=The Right Word" provides 3 simple rules—*be clear, be concise, be complete*—toward drafting better contracts.

The March 2005 newsletter presented the "dark side" of arbitration and suggested a mediation alternative that provides a viable alternative dispute resolution (ADR) mechanism that preserves the elements that distinguish the U.S. legal system.

"Data Processors, Forced to Reevaluate Pricing Strategies?"—the December 2004 newsletter—examines the effect of changes in the length of IT agreements and in risk shifting provisions on the pricing strategies of data processors.

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