Client Alert: The 8 Gotchas of Technology Contracting – Part 4

Related Professionals

Craig R. Auge

Related Services

Intellectual Property

Technology Transactions

CLIENT ALERT | 5.20.2014

This is the 4th of 4 installments on tips when contracting for technology products and services.

Every business runs at least in part on technology – and when contracting for technology products and services, the "gotchas" don't discriminate based on size or industry.

Contracts for providing and obtaining technology establish important, often long-term, relationships. When they involve mission-critical products and services, the impact of a flawed contract can be devastating. Imagine, for example, if it became impossible for a company's customers or representatives to place orders. Or imagine if a company invested in new infrastructure and hired new personnel, only to have a related software implementation fail.

Although buyers and users are more directly affected than sellers and providers, all parties can benefit from avoiding these gotchas.

Prior installments addressed the *1st Gotcha, Using the Wrong Agreement to Structure the Deal; the 2nd Gotcha, Not Making Specifications Enforceable;* the *3rd Gotcha, Scope Creep and Billing Surprises; the 4th Gotcha, Paying for Non-Performance; the 5th Gotcha, Getting Lost in the "Bermuda Triangle" of Representations, Indemnities, and Limitations of Liability; and the 6th Gotcha, Allowing Intellectual Property and Confidential Information to Escape*.

Here are the two final gotchas:

7th GOTCHA: INADEQUATELY COVERING DATA SECURITY STANDARDS

Companies that are subject to specific legal and industry data protection and security standards – and ensure that their own measures are robust and reactive to threats – also need to ensure that their service providers are meeting those same standards.

Critical to understanding what type and level of data security you need are:

- The types of data
- Where the data will reside
- Who will touch the data

The types of data will often determine what standards and requirements need to be met. For example:

- PII (Personally Identifiable Information) - covered, for example, by different state laws on data security, protection and notice of breach
- PCI (Payment Card Industry) - credit cardholder data covered by the PCI Data Security Standards
- PHI (Protected Health Information) - covered by HIPAA and HITECH
- GLB (Gramm-Leach-Bliley Act) - covering non-public personal information held by financial institutions
- POTS ("Plain Old" Trade Secrets) - covered by state trade secrets acts

Will your data be:

- On your system?
- On your vendor's system?
- On your vendor's subcontractor's system?
- In an unidentified place in the Cloud?
- Encrypted in transit *to* and *from* the system?
- Encrypted in storage?

State and country laws vary. For example, U.S. companies doing cross-border business with European Union (EU) citizens will want to be aware of the EU's directives and regulations for data protection.

Consider obtaining relevant audit results, reports, certifications and other commitments from your vendors, such as:

- SSAE 16 - SOC 1 reports on controls over financial reporting for Sarbanes-Oxley compliance, or a SOC 2 on security, availability, processing integrity, and confidentiality
- ISO 27001 certification for management frameworks for security
- Business Associate Agreement (BAA) from a service provider with access to PHI

While a vendor may comply with applicable data security requirements without being required by the agreement, ask questions and get specific commitments.

Think of it this way: **This 7th gotcha will get you if you fail to answer the question:** ***Have I fully addressed applicable data security standards and requirements?***

8th GOTCHA: MISSING IMPORTANT EXIT STRATEGIES

Just as few like to plan for the divorce before the wedding or think of the end of a marriage before even taking their vows, few like to plan for the end of a contract before it even begins. Pre-honeymoon and excited about the prospects of receiving or selling new technology or getting a much-anticipated implementation started, it can be uncomfortable to think ahead about the end of your contractual relationship.

But walking through exit strategies and covering termination scenarios – and being sure the contract reflects those – are critical to avoiding having to stay in a bad contract and to easing later transitions to new technology.

There are three classic ways for a contract to end:

1) The term expires, without renewal

2) A party terminates when the other party breaches and fails to cure in a certain amount of time

3) A party exercises a right to terminate for convenience, usually with some notice

Some specific technology products and services concerns:

- **Software**: Software that's delivered is often licensed perpetually, but the maintenance and support that goes with it is usually annual and subject to renewal. Maintenance and support could end – either due to non-renewal, the vendor ceasing to maintain and support the software, or termination – but the license itself (as a right to continue use) could continue.
- **Subscription and On-Going Services**: For subscription models (such as many Cloud, SaaS, and ASP models) that have annual or monthly terms, does it automatically renew? Can one party unilaterally elect not to renew? If so, by what steps? Think about the timing of renewal and any increases in fees. For example, if the term automatically renews unless the customer provides notice otherwise 30 days prior, then the customer will want the provider to advise of fee increases *in advance of* the 30 days so it can factor price into its decision to renew or not.
- **Service Levels**: Assuming you've specified the performance standards (see the 4th Gotcha), such as 99.9% uptime or correcting 95% of system failures within specified timeframes, and assuming meeting these is important to you, then should termination be available if service-level failures occur? *Caution:* The termination if breach-and-fail-to-cure route usually isn't sufficient, because most particular service-level problems can be cured within the cure period (e.g., often 30 days).
- **Master Agreements**: For "master" agreements, think about the different types of expirations and terminations. For example, one statement of work may terminate due to breach, but other statements of work can and perhaps should continue. Or support for certain hardware may end, but other services can continue. Or a hosting arrangement could start and stop, but not impact other services or products provided by different schedules to the master agreement. *Ask:* What do you need at any one point in

time, and how do the various components of services and products interrelate?

- **Data**: When the agreement is over, will the data be destroyed or returned? If returned, how soon and in what format? Will the old vendor cooperate to transition the data to the new vendor?

While tempting to view this as a place in the contract where provisions should apply in the same ways to both parties, that isn't commercially reasonable. Vendors and customers should be prepared to sculpt their respective termination and expiration provisions to fit their unique needs.

These are bad times to realize that you've not addressed exit strategies:

- In the throes of a breach dispute
- In a short window of time to decide to renew at a high price or be forced off a product on which you've become dependent
- In a gap between the end of the old services and before the new services can begin

Think of it this way:* This 8th gotcha will get you if you fail to answer the question: *How do I get out of this contractual relationship?

This is the last installment of this series. In sum:

This Gotcha of technology contracting . . .

. . . will get you if you fail to answer the question:

1.

Using the Wrong Agreement to Structure the Deal

What is it, and does the agreement reflect that?

2.

Not Making Specifications Enforceable

What is it supposed to do?

3.

Scope Creep and Billing Surprises

How has it changed, and have the changes and their consequences been documented?

4.

Paying for Non-Performance

Have performance standards been established, and, if so, what happens if they're not met?

5.

Getting Lost in the "Bermuda Triangle" of Representations, Indemnities, and Limitations of Liability

What's my maximum recovery if the other party breaches, and what's my maximum liability if I breach?

6.

Allowing Intellectual Property and Confidential Information to Escape

Have I sufficiently protected my intellectual property and confidential information?

7.

Inadequately Covering Data Security Standards

Have I fully addressed applicable data security standards and requirements?

8.

Missing Important Exit Strategies

How do I get out of this contractual relationship?

For more information, please contact Craig R. Auge at crauge@vorys.com or 614.464.5684.