

# With Proper Leadership You Can Do SaaS Deals Without Pain

- ◆ Mark Grossman, Attorney
- ◆ Author of the Book, “Technology Law – What Every Business (and Business-Minded Person) Needs to Know”
  - ◆ Offices in Manhattan and South Florida
  - ◆ Blog at [www.eComputerLaw.com](http://www.eComputerLaw.com)
    - ◆ Twitter @TechLaw27

# The Industry Should be Embarrassed

- ◆ Most contracts that I see are horrible
- ◆ They are not so much one-sided as incompetently drawn
- ◆ The failure to address basic questions helps nobody
- ◆ Breeding ground for litigation

# License vs. Service

- ◆ Amazing how many Vendor forms contain software license terms
- ◆ You're getting a subscription to the service and a right to use, NOT a license to the software
- ◆ No access to source or object code
- ◆ Contingency planning is what Frank discussed

# Single-Tenant Architecture

- ◆ Single-tenancy - a separate instance of SaaS software and supporting infrastructure used by each Vendor customer (tenant)
- ◆ Many more options available to the Customer in a single tenant environment
- ◆ Allows for customization
- ◆ Used by companies who need a customized approach or higher level of security
- ◆ Feels more like co-lo in many ways

# Multi-Tenant Architecture

- ◆ Multi-tenancy - a single instance of the SaaS software runs on a server and serves multiple Vendor customers (tenants)
- ◆ With multi-tenant you will have to move with the herd
- ◆ Data from multiple companies is stored on the same server
- ◆ Standard SaaS architecture results in the same configuration for all Vendor customers
- ◆ Limited or no ability to make customizations
- ◆ Suits customers who want to use the SaaS "out of the box"
- ◆ Updates at inconvenient times

# Data Ownership

- ◆ You should make no assumptions
- ◆ You should not rely on intellectual property law
- ◆ Your agreement must be crystal clear about data ownership
- ◆ Confidentiality of the data
- ◆ Destruction of the data after the agreement is over

# Getting Your Data Back

- ◆ Vendor may require a limited license to use your data as part of maintenance and monitoring your use of the service; provided, however, that Vendor complies with your privacy requirements
- ◆ However nothing in your agreement should grant Vendor an ownership interest in your data
- ◆ Instead, you should have explicitly data security requirements on how Vendor will store, transmit, restrict access to your data
- ◆ Ensure you receive all your data upon termination in a usable format

# Vendor Responsibility for Lost, Stolen, or Compromised Data

- ◆ Your contract must allocate the risk
- ◆ Somebody is going to get hurt if one of these things happen and it all boils down to who is going to take the financial loss
- ◆ You must consider your limitation of liability and indemnity clauses
- ◆ Consider backup requirements and security audits



# Bad Things Happen; Protection

- ◆ Where are the servers and your data located?
- ◆ Do you need them to remain in the US?
- ◆ Limit the Vendor employees and subcontractors who have access to your data
- ◆ Restrict Vendor moving to another datacenter without your prior approval
- ◆ Review your Vendor's disaster recovery plan
- ◆ Vendor indemnity for datacenter security breach

# Data Security

- ◆ “Vendor shall establish and maintain safeguards against the destruction, loss, or alteration of Customer data in the possession or control of Vendor which are no less rigorous than those maintained by Customer as of the Effective Date and are no less rigorous than those maintained by Vendor for Vendor’s own data of a similar nature. Vendor shall document such safeguards in writing.”
- ◆ “Vendor shall implement and maintain current industry state-of-the-art anti-virus measures to detect, prevent and remove viruses and other contaminants designed to damage, alter, delete, disable, or permit unauthorized access to, Customer’s databases, systems, equipment or property to or from Vendor’s equipment, and to prevent the spread of computer viruses between the parties which access or exchange data or software through any network connectivity.”

# Vendor Disaster Recovery

- ◆ “Vendor shall develop and execute contingency planning and disaster recovery practices consistent with the Disaster Recovery and Business Continuity Plan attached to this Agreement and Customer’s policies, business requirements, and regulations.”
- ◆ “Customer shall, from time to time, review and modify the Disaster Recovery and Business Continuity Plan and Customer policies, business requirements, and regulations, and provide modifications that shall be implemented by Vendor.”
- ◆ “Vendor shall test the Disaster Recovery and Business Continuity Plan using techniques approved by Customer.”

# Service Level Agreements (SLAs)



- ◆ SLAs are about the most important part of a SaaS deal
- ◆ If you do not specify a service level, you will not have much to push back with if the service is not what you expected
- ◆ You want credits (not penalties) if a service level is not met
- ◆ SLAs with teeth are hard to negotiate, but not impossible

# What are the Norms on Limitations of Liability?



- ◆ Most agreements have a common norm for these types of clauses
  - ◆ **“No matter what we do and no matter how bad it is, we owe you very little money and you owe us your first born.”**
- ◆ Courts aren’t in the business of rewriting contracts
  - ◆ That’s what negotiation is for!!
  - ◆ Don’t be oversold and overwhelmed by “industry norm” and their “form”

# Limits of Liability -- Typical Pro-Vendor Form

- ◆ “Vendor shall have no liability with respect to its obligations under this agreement or otherwise for consequential, exemplary, special, incidental or punitive damages even if it has been advised of the possibility of such damages. In any event, the liability of Vendor to Customer for any reason and upon any cause of action shall be limited to the lesser of the amount paid to Vendor under this Agreement or \$\_\_\_\_. This limitation applies to all causes of action in the aggregate, including without limitation to breach of contract, breach of warranty, negligence, strict liability, misrepresentations, and other torts.”

# Limits of Liability -- From Customer's Perspective

- ◆ Shoot for the full amount of the contract or more, and exclusions
  - ◆ ANY THIRD PARTY CLAIM FOR: (i) PHYSICAL PROPERTY DAMAGE; (ii) INTELLECTUAL PROPERTY INFRINGEMENT; OR (iii) PERSONAL INJURY
  - ◆ ANY CLAIM INVOLVING AN INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS
  - ◆ ANY INDEMNITY OBLIGATION PURSUANT TO THIS AGREEMENT
  - ◆ ANY CLAIM INVOLVING A BREACH OF THE CONFIDENTIALITY OBLIGATIONS SET FORTH IN THIS AGREEMENT
  - ◆ ANY CLAIM INVOLVING VENDOR'S GROSS NEGLIGENCE, RECKLESSNESS, WILLFUL MISCONDUCT, OR INTENTIONAL BREACH OF THIS AGREEMENT
  - ◆ ANY CLAIM INVOLVING A VIOLATION OF LAW
  - ◆ VENDOR'S OBLIGATIONS TO PAY OR PROVIDE CREDITS UNDER THIS AGREEMENT

# How Should You Handle Privacy Issues?

- ◆ The theme continues
- ◆ You deal with privacy issues with explicit contract provisions
- ◆ Who is legally responsible for compliance with the law?
- ◆ U.S. has few privacy laws
- ◆ Data breach statutes
- ◆ E.U. and safe harbor



# PII in SaaS Deals

- ◆ Personally identifiable information (PII)
- ◆ One of the major headaches in SaaS deals
- ◆ Require encryption of PII in transmission and at rest
- ◆ Require Vendor compliance with all applicable data protection and privacy laws and your own policies and procedures

# Language for PII in SaaS Deals

- ◆ “In the event that Customer's Confidential Information contains any PII of Customer's employees or customers Vendor agrees to comply at all times with (and maintain and safeguard such information in accordance with): (i) Customer's then-current privacy policies and procedures, and (ii) any and all applicable privacy laws, regulations, statutes, and guidelines.”
- ◆ “Vendor shall not use or disclose PII without Customer's and the employee's or customer's prior written consent. In the event that Customer and the employee or customer so consents, Vendor may disclose such PII only to the extent expressly permitted by such employee or customer and only in accordance with the terms of this Agreement and applicable law.”

# Chronic SLA Failures

- ◆ What should happen in the event the Vendor suffers chronic SLA failures?
- ◆ Chronic failures of critical SLAs--don't get lost in the weeds of making chronics apply to failures of all SLA failures
- ◆ What SLAs are the most important to you? Those become the "critical" SLAs
- ◆ Credits are not enough, at some point you should have a termination right
- ◆ But should you be able to terminate the entire Agreement or just the applicable SOW?

# Chronic SLA Failure – SOW Termination Right

“In the event Vendor, with respect to any Statement of Work, experiences four (4) or more service level failures with respect to the same critical service level within a rolling six-month period, then Customer may terminate the Services under the applicable Statement of Work as of a date specified in the notice of termination, without cost or penalty and without payment of any termination fees by Customer.”

# Transition Services

“Upon expiration of this Agreement (except where Vendor has terminated for cause), Vendor shall, at Customer’s written request, continue to provide services to Customer for a transition period of up to six (6) months after such expiration or termination at the rates and charges, and pursuant to the other terms and conditions, set forth in this Agreement as of the date of expiration. Customer shall pay all accrued but unpaid charges, including early termination charges, if any, incurred through the date of such expiration or termination. During the transition period, Customer shall not be subject to any minimum volume, usage requirements, or other commitments. During the transition period, a successor vendor may be retained to provide services to Customer. During Customer’s migration to a successor vendor following the expiration or termination of this Agreement, Vendor shall reasonably cooperate with Customer and the successor vendor in the development and execution of a plan for the orderly and efficient transition to the successor vendor.”

# Letter of Intent

- ◆ A/K/A MOU, Expression of Understanding, Agreement in Principle, and other names
- ◆ Can be binding agreements notwithstanding the name
- ◆ Be cautious
- ◆ Often a side show

# Negotiating Strategies

- ◆ 5 P's
  - ◆ Prior planning prevents poor performance
- ◆ Information is power
- ◆ Listen
- ◆ Drop the outrageous idea early

# Team Negotiating



- ◆ The “Godfather” story
  - ◆ Never disagree in public
  - ◆ Divide and conquer
  - ◆ The person stating the position must change



Mark Grossman

Tannenbaum Helpern Syracuse & Hirschtritt  
(212) 508-6748

MG@eComputerLaw.com

- ◆ To subscribe to my TechLaw blog, please give me your card
  - ◆ Blog at – [www.eComputerLaw.com](http://www.eComputerLaw.com)
  - ◆ “Technology Law – What Every Business (and Business-Minded Person) Needs to Know” available at Amazon.com or <http://tinyurl.com/ye52kou>