



COUNSEL TO GREAT COMPANIES

# Cloud Computing Legal Issues

## Practising Law institute 2021

San Francisco  
New York  
Chicago

Peter J. Kinsella  
303/291-2328

# Disclaimer

**This presentation is for educational purposes only and does not constitute legal advice. If you require legal advice, you should consult with your attorney.**

**The information provided in this presentation does not necessarily reflect the opinions of Perkins Coie LLP, its clients or even the author**

# Polling Question

1. Have you ever negotiated a cloud services agreement on behalf of a:

- a) Service Provider
- b) Customer
- c) Both
- d) Neither

# License vs. Services

- Compare:
  - Vendor hereby grants customer a non-exclusive right to use the software/services.
  - Vendor will provide Customer, in accordance with the Service Level Agreement, non-exclusive access to the Services.

# Goods/Software vs. Services Models

- Software licenses are governed by the UCC while pure service agreements are not.
  - UCC imposes implied warranties on delivered software.
    - No such warranties in a pure services contract.
  - **Less decisions concerning Unconscionability and Failure of Essential Purpose in a pure service setting**
- Contract Acceptance - Mirror Image Rule Applies to Service Agreements
  - Requires that acceptance be on precisely the same terms as the offer.
  - UCC rejects common law “mirror image” rule, as valid contracts between merchants can be formed without all terms matching doesn’t apply.

# Pricing/Payment

- Many vendors will seek payment in advance (may need to address refund issues for certain breaches and termination issues) or multi-year arrangement with monthly payments.
- Pay for use - How is “use” determined?
  - Actual use/number of users/number of employees
- Price Increases
- Benchmarking
- MFN

# Services Description

## What is included in the description ?

- Specifications?
- Published materials? FAQs?
- Bug and technical reports?

**Common Rule of Thumb:** A more detailed description of services is typically better than a description with less detail.

- It reduces arguments about whether a failure has occurred.

# Service Evolution

## What is the process for changing the Services?

- Can the customer refuse or delay a change?
- How much notification needs to be given?
  - Different notice periods for routine vs. emergency changes?
- Will a test environment be provided prior to implementing a change?
- How does pricing work?
- Are the number of changes in a given time (e.g., six month period) limited?



# Example Change Notice Obligation

Vendor will provide at least thirty (30) days advanced notice to Customer (via e-mail to Enterprise Customer Administrator(s)) **of any material changes to the Service** (each, a “**Modification**”) and permit Customer **to test such Modification in its Sandbox** for such time. If Customer objects to Vendor in email or other written form to a Modification within thirty (30) days of the date it is first identified to Customer and Vendor nonetheless proceeds or already has proceeded with the applicable Modification, Customer will have the right to terminate this Agreement as set forth in...

# Sandbox provisions

**“Sandbox”** means the non-Production testing and development environment and any ancillary environment(s) provided by Vendor to Customer for access to the Service;

**“Service”** means the provision by Vendor of an online, web-based service for access and usage by Customer via designated production and Sandbox services and associated offline components such as toolkits, programs, and other desktop utilities ....

# Service Level Agreements

- Sets expectations between vendor and customer
  - An SLA may provide an objective basis for determining whether the service is deficient.
- May establish remedies for service failures such as procedures and service credits

# Common Topics Addressed in SLAs

- Scope of Services
- Hours of support (basic vs. extended hours)
- Error reporting mechanisms
- Resolution efforts and time frames
  - Escalation
  - Metrics
- Credits
- Reporting and Management

# Common Customer Obligations when an Error has Occurred

- Validate and attempt to recreate the issue.
- Report the problem.
- Provide additional analysis and reasonably cooperate with vendor to resolve the issue.

# Service Metrics - 1

- How are service metrics defined?
  - Does entire service have to be unavailable or only particular portions?
- How are service metrics reported?
  - Does the customer need to have access to vendor tools to understand or obtain metrics?
  - Does the customer need to complain to get the credit?
- Is there a process for strengthening service metrics over time?
- Are service credits the sole and exclusive remedy arising from a performance breach?

# Service Metrics -2

- Multiple service metrics can be measured, not just service uptime. For example:
  - time between reporting a problem and acknowledging the report (response time)
  - incidents resolved in time (resolution time)
  - data bandwidth and latency issues
  - timeliness of reports
  - reporting and meetings

# Example of “Downtime” Definition

- **“Downtime”** means any period, [greater than ten minutes], within the Scheduled Available Time during which the Customer is unable to access or use the Service because of an Error, excluding any such period that occurs during any Scheduled Downtime.
- **“Scheduled Downtime”** means: (i) \_\_\_\_ hours per [day][week][month] from \_\_\_\_\_ to \_\_\_\_\_ [Day/time zone], [and, (ii) the time period identified by Vendor in which it intends to perform any planned upgrades and/or maintenance on the Service or related systems and any overrun beyond the planned completion time.]
  - Is notice needed prior to scheduled downtime?



# Exemplary Definitions of “Error”

- More Vendor Friendly: “**Error(s)**” means any failure of the Service that renders the entire Service unavailable.
- More Vendor Friendly: “**Error(s)**” means the material failure of the Service to conform to the material specifications.
- More Customer Friendly: “**Error(s)**” means any event occurring within or caused by a component of the Service that causes or is likely to cause a disruption to the Service **or any part of the Customer’s operations (including services provided to Customers).**

# Example – Error Exclusions

- Unauthorized modification of the Service –**by whom?**
- Third party hardware or software issues – **on what side of the demarcation?**
- Improper operation by customer
- **Services, circumstances, or events beyond the reasonable control of the Vendor**
- **Any issue if a customer has outstanding past due amounts**

# Resolution Times

Priority Level	Target Resolution Time
Level 1 – Major	Within 48 Hours of Acknowledgement
Level 2 – Significant	Within 5 Business Days of Acknowledgement
Level 3 – Restricted	Within 20 Business Days of Acknowledgement
Level 4 – No Impact	Will be Determined by Action Plan

Consider whether the resolution times are aspirational goals or firm contractual commitments.

# Sample Credit Calculations

## Uptime Credit Mechanism (Availability Example)

Availability Percentage (during a Contracted Month)	Compensation (% of monthly subscription fee* for contracted month that is the subject of a claim)
98.0% - 99.2%	5%
97%-97.999%	7.50%
96%-96.999%	10.00%
95%-95.999%	12.50%
94%-94.999%	15.00%
93%-93.999%	17.50%
Less than 93%	20%

# Sample Support Scorecard

## Priority 1 (High)

<b>Targeted Initial Response Time</b>	within one (1) hour of the receipt of an Incident Report
<b>Targeted Repair period</b>	[X] hours from the time of Acknowledgment.

- **Note:** Use of the word “Targeted”
- **Issue:** Does a workaround constitute a valid repair?

# Sample Credit Calculations - 2

## Mechanism Involving Multiple Factors

<b>Number of Key Performance Metrics (KPIs) breached in applicable reporting period</b>	<b>Service Credit percentage of the monthly Support Service Fee</b>
<b>Breach of one (1) KPI</b>	4 %
<b>Breach of two (2) KPI</b>	8 %
<b>Breach of three (3) KPI</b>	16 %
<b>Breach of four (4) KPI</b>	32 %
<b>Breach of five (5) KPI</b>	64 %

# Termination Right for failing to meet SLA

- What severity levels count towards termination? (Severity 1, Severity 2?)
- How many issues need to occur in what period of time?
  - 2 in 6 months?
- Is there a right to terminate if issue lasts beyond a certain amount of time?
  - Severity 1 isn't resolved within 24 hours?
  - Severity 2 isn't resolved in 48 hours?

# What is the process for reporting and fixing errors?

- How is a problem reported?
  - E-mail? Website? Telephone call?
- What information is submitted?
  - Description of incident?
  - Requested severity level?
- What is the process for determining that a problem has been fixed?
  - When the customer or vendor says it is fixed?
- When does the clock start and stop?



# Reporting Procedures

- What reports does the vendor supply?
  - Usage Statistics?
  - Errors?
  - Downtime?
  - Resolution?
  - Root Cause Analysis?
- When are the reports supplied??

# End User Conduct

- Contracts often allow the vendor to suspend or terminate service for bad user conduct (and for other reasons).
- The customer will want to make sure that such right may only be exercised in well-defined situations, preferably with advanced notice. The customer will want to limit suspension:
  - To breaches that significantly threaten the security or integrity of the cloud service
  - To the user accounts in which the breach occurred, rather than all of customer's accounts

# Exemplary Cloud User Restrictions

Customer will not: (i) use the Service in violation of applicable Laws; (ii) send or store infringing, obscene, threatening, or otherwise unlawful or tortious material, including material that violates privacy rights in connection with the Service; (iii) send or store Malicious Code in connection with the Service; (iv) damage, disable, overburden, impair, interfere with, or disrupt the Service; (v) attempt to gain unauthorized access to any systems or networks that connect thereto or otherwise interfere with the operation of the Service or in any way with the use or enjoyment of the Service by others; (vi) permit more users to access or use the Service than are permitted in the Order Form; (vii) allow more than one individual to use a user account; (viii) make the Service available to any third party (via a services arrangement, service bureau, lease, sale, resale, or otherwise); and, (ix) exceed any applicable bandwidth limit or storage capacity limit, if any.

# Exemplary Cloud User Restrictions (edited)

Customer will: (i) not use the Service in violation of **Laws applicable to Customer**; (ii) **not knowingly** send or store infringing, obscene, threatening, or otherwise unlawful or tortious material, including material that violates privacy rights in connection with the Service; (iii) **use commercially reasonable efforts to prevent sending or store** Malicious Code in connection with the Service; ~~(iv) damage, disable, overburden, impair, interfere with or disrupt the Service~~; (v) **not knowingly** attempt to gain unauthorized access to any systems or networks that connect thereto ~~or otherwise interfere with the operation of the Service or in any way with the use or enjoyment of the Service by others~~; (vi) **not** permit more users to access or use the Service than are permitted in the Order Form; (vii) **not authorize** more than one individual to use a user account; (viii) not make the Service available to any third party (via a services arrangement, service bureau, lease, sale, resale, or otherwise), **except with respect to contractors and customers of Company**; and, (ix) **not knowingly**, exceed any applicable bandwidth limit or storage capacity limit, if any.

# Common Data Issues

Define "data"

- Stored data, usage metrics, aggregate or de-identified data?

Specify ownership rights in the data

Specify purposes for which the data may be used

- Is the vendor permitted to use the data (or aggregate data) for other purposes?

Vendors will typically want warranties from the customer concerning ability to have vendor process customer information.

# Data Ownership – Pro-Customer Vendor Restrictions

To the extent that any Personal Data is collected or accessed through the Services, Customer owns all right, title, and interest to all such Personal Data, and Vendor will: (a) not use or collect Personal Data for any purpose other than as necessary to perform Vendor's obligations under this Agreement; (b) treat Personal Data as Customer Confidential Information in accordance with the confidentiality provisions of this Agreement [**Note - Does confidentiality provision have separate PII Clause?**]; (c) not disclose Personal Data except as expressly permitted in this Agreement; and, (d) keep all Personal Data compartmentalized or otherwise logically distinct from, and in no way commingled with, other information of Vendor or its employees, suppliers, customers, or other third parties.

# Sample Prohibition on Data Transfer

Vendor covenants during the Term of this Agreement that: (i) Customer Data will not be transferred or exported outside of the United States; (ii) Vendor will perform the Services hereunder using data centers solely located within the United States; (iii) any and all Services provided to Customer under this Agreement, including but not limited to technical support, will be provided from within the United States. [address foreign nationals?]

# Sample Data Return and Destruction Clause

Upon the earlier of Customer's request or the expiration or termination of this Agreement, Vendor will provide Customer with all Customer Data contained in the Services or otherwise in the possession or control of Vendor in a format and media reasonably acceptable to Customer.

Question: When is data actually deleted?

Recommendation: Best to be precise



# Data Access – sample provision

Customer will have unrestricted access to, and has the right to review and retain, the entirety of Customer Data contained in the Services or otherwise held by Vendor, including all computer or other files containing Customer Data. At no time will any such files be stored or held in a form or manner not immediately (if retained online) or promptly (if retained in another medium) accessible. Vendor will provide to Customer all passwords, codes, comments, keys, and documentation necessary for such access and as necessary to utilize the Services. **Without limiting the generality of the foregoing, Vendor will comply with the Data Access Rider attached hereto as Exhibit D.**

# Underlying Hosted Service/Co-Location Issues -1

Can the vendor use an underlying hosted service or co-location center and still comply with its customer's SLA obligations?

- Consider:
  - Response times
  - Reporting obligations
  - Subcontracting and assignment provisions

Does the vendor have sufficient recourse against the Data Center?

- Will the vendor pay the customer more credits than it will receive? (not an atypical situation)

# Underlying Hosted Service/Co-Location Issues -2

## Does the vendor:

- have a business continuity plan?
- provide redundant operations from different sites?
- routinely test its back-up capability?
- routinely attempt to restore data?

It is important to consider the impact of bankruptcy on the ability to access data and the ownership of back-up media.

# Security Events

- Agreements may distinguish between "Security Issues" and "Security Incidents" and provide different rights, obligations, and remedies for each category.
- Security Issues – issues that could give rise to a security breach
- Security Incidents – actual breach of security

# Security Issues

- How are security issues defined?
  - Objective vs. subjective definition
  - Are issues in the vendor's control and those in the control of its subcontractors differentiated?
  - Does every problem need to be investigated?
  - Does every problem need to be fixed?
- What is the process for fixing the issue?
  - Is there a specified time frame?
  - How is the time frame adjusted for fixes that take longer to implement?

# Security Incident

- Notice requirement to other party
- Remediation efforts
  - Who does what?
  - Who pays for the remediation efforts?
  - Does the breach require end-user notification?
- Who has legal liability for the incident?
  - May want to address liability caused by third parties (e.g., hackers)

# Data Retention Issues

- Customers may want two conflicting obligations.
  - Vendor should keep the data as long as customer needs it.
  - Vendor should promptly destroy it when it is no longer needed.
- Depending on the service, vendor may not know the content of the data.
- **Contract should specify when data is destroyed.**

# Compliance Requirements

- Customer may want the contract to contain procedures for auditing compliance issues:
  - Does the vendor data center facility allow visitors?
  - Will the audit disclose too much security information?
  - Will a customer's auditor have access to other customers' data?
- Customer may want to impose compliance obligations on the vendor.



# Confidentiality Clauses

- May impose a back door security obligation on the vendor.
  - Is the vendor obligated to keep a customer's information protected from unauthorized access use or disclosure?
- **Compare:**
  - Vendor will not copy, disclose, or permit unauthorized access, use or disclosure of Confidential Information.
  - Vendor will keep all Confidential Information confidential.
  - Vendor will use commercially reasonable efforts to protect Confidential Information.

# Subcontractors -1

- Are subcontractors used to provide the service?
  - Does the vendor have power to impose contractual obligations on the subcontractors?
  - Are flow down obligations required under law (e.g., HIPAA, GDPR)?
- Can vendor identify the subcontractors?
- Does the customer have a right to approve new subcontractors? Or a termination right?
  - What is the approval/disapproval process?
  - Vendors are very reluctant to provide approval right, but may provide a termination right.

## Subcontractors -2

Vendor will not subcontract or otherwise delegate all or any portion of its obligations under this Agreement to any third party (“**Subcontractor**”) without Customer’s express written consent. Vendor will ensure each Subcontractors’ compliance with the terms of this Agreement and will be liable to Customer for any act or omission of a Subcontractor to the same extent Vendor would be liable had the Vendor committed such act or omission.

# Disaster Recovery - 1

Does the vendor:

- have a business continuity plan?
- provide redundant operations from different sites?
- routinely test its back-up capability?
- routinely attempt to restore data?

What events cause the vendor to engage in data recovery operations?

# Disaster Recovery - 2

- Does the contract contain data recovery goals?
- What are the consequences if the data is not recovered within the specified time frames?
- Who takes priority if multiple vendor customers are affected?
- How will a Force Majeure event impact contractual obligations?

# Disaster Recovery Plans

Vendor will maintain during the Term, a Business Continuity Management Program that includes all aspects of Business Continuity Planning and Disaster Recovery Planning. The Business Continuity Management Program and the resulting Business Continuity Plan will cover all the Services to be performed under this Agreement. Vendor will provide Customer with the opportunity to review and evaluate the Business Continuity Management Program, including the Business Continuity Plan and will remediate any findings. Such review and evaluation may include participation in Customer's: (a) vendor testing and assessment process including the completion of online and/or on-site assessment(s), as appropriate; and, (b) recovery testing of a mutually agreed upon scope and frequency. Vendor will conduct at least annual internal information security audits of its Business Continuity Plan and certify the results of each such audit to Customer within ten (10) days of completing each such audit.

# Disaster Response

Notwithstanding Section [X] [FME Clause], in the event of a disaster or any other disruption event that prevents or impairs Vendor from performing the Services, Vendor will notify Customer and immediately implement its Business Continuity Plan to restore and continue providing the Services to meet the Recovery Objectives. Upon cessation of the disaster or disruption event, Vendor will, as soon as reasonably practicable, provide Customer with an incident report detailing the reason for the disaster or disruption and all actions taken by Vendor to resolve the disaster or disruption.

# “Force Majeure” - Foreseeability - 1

There is significant variability between jurisdictions as to whether a Force Majeure event must have been unforeseeable at the time the contract was formed.

Some courts have held that a nonperforming party may not be able to rely on a force majeure clause where the claimed event was foreseeable to the parties at the time the contract was formed. Some states will impute this test on the entire clause if it is silent on foreseeability. Other states will only apply this test to the catchall provisions and not to specific triggers.

*Example, **TEC Olmos, LLC & Terrace Energy Corporation F/K/A Terrace Resources, Inc. v. ConocoPhillips Company**, No. 01-16-00579-CV, slip op. (Tex. App.—Houston [1st Dist.] May 31, 2018). [On next Slide]*



# “Force Majeure” - Foreseeability - 2

In the *TEC* case, the contract had the following language:

**FORCE MAJEURE:** Should either Party be prevented or hindered from complying with any obligation created under this Agreement, other than the obligation to pay money, by reason of fire, flood, storm, act of God, governmental authority, labor disputes, war *or any other cause not enumerated herein but which is beyond the reasonable control of the Party whose performance is affected*, then the performance of any such obligation is suspended during the period of, and only to the extent of, such prevention or hindrance, provided the affected Party exercises all reasonable diligence to remove the cause of force majeure. [emphasis added]

The clause lists seven specific events, followed by the catch all provision. The court held that unforeseeability was a requirement to excuse performance under the catch-all provision, but not the specified **force majeure** trigger events.

# Sample Force Majeure Clause -1

**Force Majeure.** Except as expressly set forth in Section [X], the obligations of Vendor under this Agreement will be suspended during the period and to the extent that Vendor is prevented or hindered from performing any such obligation due to any cause beyond Vendor's reasonable control, regardless of whether such cause is foreseeable (such a cause, a "**Force Majeure Event**"), including any: (i) act of God; (ii) flood, fire, explosion, natural disaster; (iii) act of terrorism, war, invasion, riot or other civil or military disturbances; (iv) act, regulation, or law of any government, civil or military authority; (v) embargo, blockade, tariff or other trade restriction in effect on or after the Effective Date; (vi) national or regional emergency; (vii) epidemic, pandemic or other contagion, including COVID-19; (viii) strike, labor stoppage or slowdown or other industrial disturbance; (ix) shortage of any supplies or services; or, (x) interruption, loss, malfunction or shortage of utilities, transportation, communications or computer software, hardware or services.

# Sample Force Majeure Clause -2

## Common proviso

... provided that the Party affected by such delay **is using reasonable commercial efforts to mitigate or eliminate the cause** of such delay or its effects and, **if events** in the nature of the force majeure event were foreseeable, **used commercially reasonable efforts prior to its occurrence** to anticipate and avoid its occurrence or effect

# Escrow Issues -1

- U.S. Bankruptcy Law 365(n) provides protection to **licensees**.
  - If licensor goes bankrupt, licensee can continue using rights.
  - The agreement language will be important for determining whether the cloud customer is a licensee
- Many foreign bankruptcy laws do not provide similar protection.
- Escrow Issue: U.S. Bankruptcy Law likely prohibits exercise of springing license grant.

**Therefore need a “present license” to use escrow materials.**

# Escrow Issues -2

- Some types of contracts may be appropriate for escrow.
  - Escrow Agents are now providing escrows for cloud applications that run in a standard environment (e.g., “app” running on Amazon or Azure platform).
- Data Escrows - Data stored with a third party that can be accessed separately by customer.
- Terms (e.g., release conditions, scope of use, etc.) can be negotiated. See next slide

# Sample Customer Favorable Escrow Release Conditions

- Vendor materially breaches this Agreement.
- Vendor becomes subject to bankruptcy proceeding or insolvency or enters into any arrangement with its creditors.
- Vendor is subject to a change of control.
- Vendor permanently ceases operation of its business.
- Others? Fails to add competitive functionality?

Vendor will want attempt to limit these release conditions.

# Risk Allocation

- Typically, the customer wants to impose a combination of the following obligations on the vendor:
  - Operating procedures (cloud)/obligations
  - Warranties/Covenants
  - Indemnities
  - Audit
  - Insurance
- Typically, the vendor wants to minimize obligations (especially any obligation that slows its ability to make changes or causes “out of process” deviations) and impose other limitations on its liability.

# Operating Procedures

- Customer will want to try to memorialize diligence results (including vendor procedures).
- DPA obligations
- Back-up and recovery procedures
- Compliance procedures
- Audit procedures



# Warranties / Covenants

- If a vendor provides warranties, they are often “soft”:
  - Compare: “Vendor will have a security policy” vs. “vendor will have and comply with its security policy”
  - Compare: “Vendor will prevent unauthorized access” vs. “ Vendor has reasonable security measures in place that are designed to prevent unauthorized access”

If a warranty or covenant is breached, it can lead to damage claims and contract termination.

# Integration clause can defeat extrinsic warranties

- Without a proper integration clause, extrinsic affirmations can be made part of a sales agreement.
  - Example: “This Agreement, including all exhibits and addenda hereto and all Order Forms, constitutes the entire agreement between the parties with respect to the subject matter hereof.”

Integration clause may not prevent fraudulent inducement claims.

# Indemnification - 1

- Indemnities
  - Vendors will typically try to provide very limited, if any, indemnification obligations.
  - Indemnification obligations will usually not trigger contract termination unless an express termination provision is linked to the indemnity.

Vendors may push to provide a capped indemnity obligation rather than a warranty to avoid termination issues for breach.

## Indemnification - 2

- Traditional exemplary indemnity clause

Vendor will **indemnify, defend and hold** Customer, its affiliates and their principals, agents and personnel **harmless** against **all** costs, fees, expenses, damages and liabilities (including attorneys' fees and other defense costs) suffered, incurred or awarded against Customer **as a result of any third party claim, suit or dispute** relating to or arising from:

# Indemnification - 3

- Defend and Pay Awarded Damages

Vendor will **defend** Customer against any third party claim, action, proceeding or suit, and **will pay** for the resulting costs and damages **finally awarded** against Customer to such third party **by a court of competent jurisdiction** or agreed to in settlement by Vendor, arising from:

# Indemnity -- Scope of Obligation

## Consider what is covered

- claims? allegations? final decisions?
- type of damages? finally awarded damages? attorney fees?
- covered activities
  - simply the existence of the product or software
  - claims directed at the “use” of the product or software
  - increased risk due to using the cloud? (data breach, privacy laws)
- what type of intellectual property rights are covered?
  - patents, copyrights, trademarks, trade secrets?

# Indemnity – Vendor's Common IP Exclusions

## What is Excluded?

- Service is configured or used in accordance with Buyer's specifications
- Licensee uses service in manner other than the normally intended manner
- Service is used in combination with software, products or procedures not provided by Seller
  - exception to exclusion - unless such product is normally intended to be used with such a product
- Service is modified or not properly maintained by Buyer
- Licensee's wilful, knowing or deliberate infringement of a patent, copyright, trade secret, trademark or other proprietary right
- The use of the services to produce other materials or equipment

# Sample Indemnity Provision—What is Covered?

Vendor will **defend at its own expense and indemnify** and hold Customer, its Affiliates, and their respective directors, officers, employees, contractors and agents (collectively, “**Customer Indemnitees**”) harmless from and against any and all claims, liabilities, losses, damages, judgments, awards, costs (including, without limitation, legal fees and expenses), actions and/or other proceedings made, sustained, incurred, brought or prosecuted **in any manner whatsoever relating to or arising from any:** (a) **actual or alleged** infringement of a third-party’s Intellectual Property Rights by the Services, Documentation **or use thereof** by Customer or its Affiliates (**in each case, either alone or in combination with other elements that are necessary to use the Services or Documentation for its intended purpose**); (b) property damage, personal injury or death to the extent caused by the negligence, willful misconduct, acts or omissions of Vendor or by its employees, contractors or agents; (c) **act or omission of Vendor**; (d) **unauthorized access, use or disclosure of Customer Data**; (e) breach of this Agreement by Vendor; (f) failure by Vendor to satisfy any of its tax or withholding obligations; or, (g) claims arising out of Vendor’s liability to its employees, contractors or agents.



# Indemnity – Conditions/Limits

Vendors may seek to impose certain conditions on obligation to indemnify Buyer:

- adequate notice of third-party claim
- limitation of the remedy
- control of defense and settlement
- cooperation of Buyer

# Categories of Damages

## Direct (basic measure of damages)

- Damages which a reasonable person would expect to naturally and necessarily result from a breach

## Incidental damages

- Expenses or commissions in connection with effecting cover and any other reasonable expense incident to the delay or breach

## Consequential damages

- Damages that arise out of special circumstances, not ordinarily predictable

# Lost Profits – Direct or Consequential? -1

Courts have held that “lost profits” can be either direct or consequential damages. Compare:

- ***Moore v. Boating Indus. Ass'ns***, 745 F.2d 698, 717 (7th Cir. 1985) (“Lost profits are considered to be general or direct damages in a breach of contract case . . . .”)
- ***Fishman Org., Inc. v. Frick Transfer, Inc.***, No. 11-cv-04598, 2013 WL 1655984, at \*3 (E.D. Pa. Apr. 17, 2013) (“Lost profits are considered a form of consequential damages.”)
- ***SOLIDFX, LLC v. Jeppesen Sanderson, Inc.***, 841 F.3d 827, 839 (10th Cir. 2016) (noting that lost profits can be either direct or consequential, depending on their nature)

## Lost Profits – Direct or Consequential? -2

Best practice from a vendor perspective - Disclaim lost profits in addition to consequential damages.

IN NO EVENT WILL VENDOR BE LIABLE FOR DAMAGES **FOR LOSS OF PROFIT OR REVENUE**, LOSS OF GOODWILL, OR ANY SPECIAL, INCIDENTAL, INDIRECT, PUNITIVE, OR CONSEQUENTIAL DAMAGES...

# Common claims that might give rise to consequential damages

- IP Infringement
- Breach of Confidentiality
- Data Security Breach
- Claims that may impact reputation (product liability etc.)

*All big concerns with the Cloud!*

# Security Breach – Deemed Direct Damages

## Exemplary Language

These following items will be classified as direct damages and will not be limited by Section [X]: (a) conducting necessary and appropriate investigative and/or forensic activities to determine if your data was subject to unauthorized access, misappropriation, damage, or destruction; (b) your reasonable costs for breach notifications to individuals whose personal information was misappropriated that you are legally required to provide; (c) your reasonable costs for twenty four (24) months of credit monitoring for such individuals; and, (d) any fines or penalties that you must pay to government entities.

# Damage Exclusion Clauses Can Backfire

*Piper Jaffrey & Co. v. SunGard Systems International, Inc.*, No. 04-2922, 2007 U.S. Dist. LEXIS 11399 (D. Minn. Feb. 16, 2007).

- Consequential damage exclusion clause in software license limited the software owner's copyright infringement claims arising from the customer's unlicensed use of the software following termination of the license agreement.
- Court rejected the argument that the copyright infringement claim arose outside of the agreement and was therefore not limited by the consequential damage exclusion clause contained in the license agreement.
- Court held that since the software company was seeking indirect damages based upon the customer's unlicensed use of the software, such damage claims were barred by the agreement's prohibition on consequential damages.

# Common Limitation of Liability Clauses to Consider

- Caps on the “type” of damages
  - Direct vs. Consequential vs. Incidental
- Caps on the “amount” of damages
  - Different categories of damages may require different amounts.
- Caps on remedies
- Exceptions to one or both of the caps?
  - See preceding slide



## Some Jurisdictions Require Limitations of Liability and Warranty Disclaimers to be negotiated

General disclaimers of negligence are disfavored and enforceable only if specifically agreed to in negotiations between a commercial seller and commercial buyer. ***United States Aviation Underwriters, Inc. v. Pilatus Bus. Aircraft, Ltd.***, 358 F. Supp. 2d 1021, 1024 (D. Colo. 2005) citing *See Hiigel v. General Motors Corp.*, 544 P.2d 983, 989-90 (Colo. 1975)

In Washington, "[d]isclaimers of warranty are not favored in the law.... [A] disclaimer or waiver of warranty is ineffective unless (1) it is explicitly negotiated between the buyer and the seller, and (2) it sets forth with particularity the qualities and characteristics that are not being warranted." ***W. Rec. Vehicles, Inc. v. Swift Adhesives, Inc.***, 23 F.3d 1547, 1554 (9th Cir. 1994) (applying Washington law) (citations omitted).

# How to address negotiation requirement?

- Make the Limitation of Liability and disclaimers mutual, with appropriate carve outs...

EXCEPT WITH RESPECT TO CLAIMS OF INDEMNITY, BREACH OF CONFIDENTIALITY, BREACH OF DATA SECURITY OBLIGATIONS, OR THE UNAUTHORIZED USE OF A PARTY'S INTELLECTUAL PROPERTY RIGHTS, IN NO EVENT SHALL EITHER PARTY BE...

- Add Basis of Bargain Language

**Basis of Bargain.** EACH PARTY RECOGNIZES AND AGREES THAT THE WARRANTY DISCLAIMERS AND LIABILITY AND REMEDY LIMITATIONS IN THIS AGREEMENT ARE MATERIAL, BARGAINED FOR BASES OF THIS AGREEMENT AND THAT THEY HAVE BEEN TAKEN INTO ACCOUNT AND REFLECTED IN DETERMINING THE CONSIDERATION TO BE GIVEN BY EACH PARTY UNDER THIS AGREEMENT AND IN THE DECISION BY EACH PARTY TO ENTER INTO THIS AGREEMENT.

- Take Phone Calls

# Economic Loss Rule -1

The rule bars plaintiffs from recovering pure economic losses under a negligence theory without personal injury, property damage or a special relationship.

“[A] party suffering only economic loss from the breach of an express or implied contractual duty may not assert a tort claim for such a breach absent an independent duty of care under tort law.” ***Town of Alma v. AZCO Constr., Inc.***, 10 P.3d 1256, 1264 (Colo. 2000). See, ***Southern California Gas Co. v. Superior Court***, No. B283606, 2017 WL 6398546 (Cal. Ct. App. Dec. 15, 2017)

The rule “prevents recovery for negligence when the duty breached is a contractual duty and the harm incurred is the result of failure of the purpose of the contract.” ***Jardel Enterprises, Inc. v. Triconsultants, Inc.*** 770 P.2d 1301, 1303 (Colo. App. 1988).

# Economic Loss Rule -2

Businesses that filed a class action against SoCalGas, asserting negligence based claims arising from a gas leak are barred from recovering negligence damages because they failed to allege any property damage or personal injury. Instead, they alleged that the gas leak and subsequent relocation of residents of the surrounding area caused purely economic injuries to their businesses. ***Southern California Gas Co. v. Superior Court***, No. B283606, 2017 WL 6398546 (Cal. Ct. App. Dec. 15, 2017)

# Economic Loss Rule -3

In some jurisdictions, the economic loss rule does not apply where the defendant owes the plaintiff a duty of care that is independent of any contractual duty. ***Town of Alma***, 10 P.3d at 1263; ***Andrews v. Picard***, 199 P.3d 6, 10 (Colo.App. 2007). See ***Rhino Fund, LLLP v. Hutchins***, 215 P.3d 1186, 1191 (Colo. App. 2008) (economic loss doctrine was inapplicable to claims under the civil theft statutes, "because the agreements [did] not address remedies in the event the collateral [was] diverted" and because ***Hutchins*** also had independent duties in tort to avoid converting the collateral proceeds).

# Negotiating thoughts from a Customer Perspective -1

- It's not enough to get a higher damage cap for contract breaches (e.g., breach of privacy obligations) if the underlying contract obligations are unlikely to be breached (e.g., "Vendor will have a privacy policy")
- Customer should strive to impose specific as well as general obligations on the vendor. (e.g., "Vendor will comply (and cause its employees to comply with) its internal and external privacy and data security policies" or "Vendor will implement and maintain all commercially reasonable measures to protect Customer Data from unauthorized access, use or disclosure")
- Try to obtain a general indemnification for the unauthorized access, use, or disclosure of Customer Data [caused by Vendor's acts or omissions / failure to take reasonable actions to protect the Customer Data / ]

# Insurance

- Contract may require a party to carry certain levels of insurance.
- CGL policy may not be enough to cover many cyber liability issues.
- Cyber liability policy may have lower limits for certain categories of damages (e.g., breach notification, credit reporting services).
- Requires consultation with broker/agent.

# Termination and Transition - 1

- Every contract will end at some time.
  - It is important to plan for termination issues prior to contract execution.
- Customer will want the agreement to address
  - Transition assistance
    - Data migration
      - Format of data?
      - It may not be easy to copy or download the data.
    - Continued provision of services until transition completed
- Vendor will want payment for early termination and for any post-termination services.



# Termination and Transition - 2

- Beware of termination obligation that includes an agreement to agree.
- Example termination obligations
  - Continue to provide services during the transition
  - Assist with transition
    - Deliver data
    - Delivery ancillary information
  - Securely destroy records

# Sample Transition Services Obligation

If this Agreement expires or is terminated for any reason, then Customer may extend the Term of this Agreement for up to an additional twelve (12) months, at Customer's request and option, from the termination or expiration date ("**Transition Period**"). During any such Transition Period, Vendor will: (a) continue to provide the applicable Services; (b) provide the additional transition services reasonably requested by Customer; (c) coordinate communications to provide for an orderly transition of the Services to Customer or another service provider designated by Customer; and, (d) work with Customer promptly and in good faith to provide for an optimal and orderly transfer of such Services, including, but not limited to assistance in transferring services, equipment, licenses, all record layouts, data, data definitions and file structures (with definitions), data files in a format reasonably requested by Customer and any and all other information, resources and materials used to perform the Services to the extent necessary for a conversion from the Services to Customer or to any new service provider selected by Customer.

# Thanks!

**Peter J. Kinsella**

**[pkinsella@perkinscoie.com](mailto:pkinsella@perkinscoie.com)**

**303-291-2300**



Peter J. Kinsella 303-291-2300