SUMMER 2013

COUNSEL FOR THE ROAD AHEAD®

InterConnect

A PUBLICATION OF BENESCH FRIEDLANDER COPLAN & ARONOFF LLP'S TRANSPORTATION & LOGISTICS GROUP

Critical Issues for Use of Cloud-Based "Infrastructure as a Service" in the Age of Security and Privacy Regulation

Are You On Track to be Compliant with the "Mega-Rule" Before Enforcement Begins on September 23, 2013?

The past few years have seen the advent of several competing trends. Transportation and logistics companies large and small have decided that it is in their best interest to move and store critical data off-site, to the "cloud," using the infrastructure provided by third parties as a service. This form of business process outsourcing, called "infrastructure as a service" or "IaaS," provides cost savings and operational efficiencies. At the same time, concerns about the privacy and security of IaaS-stored data have increased significantly, and a myriad of federal, state, local and foreign laws, rules and regulations have been enacted in response to those concerns. These competing trends mean that, while IaaS can be beneficial, it is not without risk. This article will summarize the business case for IaaS and address some of the most important issues that arise in connection with the implementation of IaaS, which can complicate an otherwise straightforward business case.

The Business Case for IaaS

The business case for moving to IaaS to support critical data storage and other information technology infrastructure needs is compelling. Many companies, including market leaders Amazon Web Services, Microsoft Azure, Terramark, Savvis, CSC, Dimension Data, Rackspace, Tier 3, SAP/SuccessFactors and IBM/Sterling Commerce, as well as lesser known regional players, and specialized players such as Lexis Data and Equifax Information Services in the financial services sector, have entered the marketplace offering IaaS and data warehousing services. At the international level, companies such as AT&T, IBM, Datapipe, Hosting.com, Tata Communications and Virtacore Systems have become recognized participants. Regardless of the geographic reach or size of the IaaS vendor, the business case for moving toward an outsourced model for infrastructure and data storage remains the same—cost and efficiency. IaaS provides transportation and logistics companies large and small with the ability to utilize the availability, scalability and cost savings inherent in third-party IaaS offerings to outsource their infrastructure needs. In addition, these companies are able to shift some of the risk inherent in managing critical infrastructure to third-party IaaS vendors contractually through service level, disaster recovery and other provisions; reduce manpower needs for infrastructure maintenance and support, or shift workers to other critical projects; and achieve increased levels of critical infrastructure redundancy and geographic diversity than they might otherwise be able to achieve without IaaS. In short, the business case for IaaS has become a compelling one—pushing internal information technology, finance

continued on page 2

One example of this arises in connection with the so-called Mega Rule—the omnibus security rule promulgated under HIPAA and the HITECH Act that became effective in March 2013 and will become effective for compliance purposes on September 23, 2013.

IN THIS ISSUE:

Benesch Attorneys at Law

Critical Issues for Use of Cloud-Based "Infrastructure as a Service" in the Age of Security and Privacy Regulation

continued from page 1

and strategy executives to consider increased use of the cloud (and IaaS vendors in particular) as sources for the expansion of critical infrastructure.

The State of the Law

As the business case for increased use of IaaS becomes more and more compelling, the legal environment, both in the U.S. and abroad, is changing rapidly. Just as IaaS becomes a global industry with a critical mass of vendors supporting customers that are large and small, public and private, we see an increased level of scrutiny and both statutory and regulatory efforts to protect data of all kinds. These efforts arise under federal, state, local and foreign laws, rules and regulations, which, in their attempts to protect against privacy and data security breaches, substantially increase the risk associated with the use of IaaS (and its cousins, software as a service, or SaaS, and platform as a service, or PaaS). In the years since the advent of cloud-based computing systems and platforms, the law, both domestic and foreign, has expanded exponentially. In the United States, where the privacy and security law is largely sectorial in nature (i.e., governing particular industries or types of data deemed to be particularly sensitive, such as financial information, protected health information and information pertaining to children), the last few years have seen a torrent of new laws and regulations.

These include specific laws and regulations pertaining to data security and privacy at the state and local levels; new omnibus regulations governing the security of protected health information; new regulations governing the privacy and security of information gathered from children; statutes and regulations governing the privacy and security of consumer financial information; and federal and state data breach disclosure laws and regulations. The applicable laws, rules and regulations are widely known by their sponsors' names or acronyms, including Gramm-Leach-Bliley or GLB, HIPAA, HITECH, COPPA, Sarbanes-Oxley and "Red Flag," to name a few. Several bills are currently pending in Congress that could further alter the legal landscape in the United States by establishing a national data security standard.

Internationally, the major industrialized nations of the world are far ahead of the United States in terms of the omnibus approach they take to preserve and protect the privacy and security of information. The European Union nations and Switzerland alone have passed expansive legislation in compliance with EU directives on privacy, security, eCommerce, distance selling and the use of "cookies" and other devices that impact the privacy of personal information. The European directive pertaining to data security and the cross-border transmission of personal information is undergoing a substantive overhaul, with final rules expected in the coming months. Other nations, including Canada, Australia, Mexico and the major industrialized nations of Asia, have followed suit by promulgating extraordinarily stringent privacy and security laws and regulations that apply to cross-border data transmissions.

Oftentimes, the laws, rules and regulations imposed on companies seeking to transfer data to third-party data centers and utilize IaaS provide onerous yet conflicting requirements on companies. Many of the laws, rules and regulations pertaining to data security contain either explicitly required data security standards or recommended guidelines. For example, the recommended security standards under HIPAA and HITECH are the standards published by NIST, while the recommended security standards under the data security laws of the European Union and Switzerland are the ISO 27000 standards. To further complicate matters, in the United States (other than under HIPAA and HITECH), the applicable required or suggested privacy and data security standards and guidelines include guidelines promulgated by the Federal Trade Commission and the PCI Data Security Standard, or PCI DSS.

One example of this arises in connection with the so-called Mega Rule—the omnibus security rule promulgated under HIPAA and the HITECH Act that became effective in March 2013 and will become effective for compliance purposes on September 23, 2013. This rule alone spans hundreds of pages and essentially requires that entities that were never originally intended to be brought within the purview of HIPAA security compliance comply in full with the intensive security rules under HIPAA and HITECH. These include entities that are far afield of any connection to healthcare or the provision of health services, such as transportation and logistics companies with self-insured health insurance plans and service providers that do business with such companies and store or process employment data that includes protected health information. Companies that now find themselves covered by the Mega Rule and desire to utilize IaaS for the storage of employment data that includes protected health information must, therefore, ensure that the IaaS vendor(s) with which they contract are in turn Mega Rule compliant. Some are…many are not.

A further example arises under the federal Sarbanes-Oxley Act, which applies by its terms to public companies (and certain private companies) under the federal securities laws. Under Sarbanes-Oxley and the rules promulgated thereunder, applicable companies are required to certify

annually to their internal controls as part of the certification of the accuracy of the financial data incorporated into their public filings—the theory being that without adequate controls, the accuracy and integrity of financial data could be in doubt. As part of the process of maintaining adequate controls, ensuring data security is paramount. As a result, companies seeking to utilize IaaS routinely demand specific security-related audit information from vendors, including SSAE 16 (SOC 2) type 2 reports or equivalent audit reports, and to provide indemnity for data security lapses and breaches.

In the real world of technology transactions, the net effect of this is to significantly increase the costs associated with the provision of IaaS, as vendors seek to limit their risk contractually or are forced to insure against increased risk. As part of their own compliance obligations, companies have no legal choice but to require that IaaS vendors comply in full with applicable law and attempt to pass the risk associated with these requirements on to the IaaS vendors with which they contract (though this may involve compliance with several different technical standards). All of this adds substantially to the complexity and cost of adopting IaaS, even when the basic business case favors it.

Conclusion

The business case for IaaS is clear, but the domestic and foreign legal environment is complex, changing and often in conflict. Transportation and logistics companies looking to charge forward into more expansive use of the various forms of cloud-based business process outsourcing, including IaaS, SaaS and PaaS, must do so with their eyes wide open to the issues and risks associated with a legal environment that is not always in step with the desire to take advantage of the positive attributes of the cloud.

For more information, please contact Michael D. Stovsky at mstovsky@beneschlaw.com or 216.363.4626.

Customs POA: 5 Simple Things to Consider

Our firm has already received numerous Customs power of attorney (POA) questions this year. This is a good thing, as it means that folks are doing things the right way. If you import, you already know that any violation of Customs law can be very expensive. If you have not yet begun to import, then you should know that any Customs violation can be very costly. While there are many things to consider with regard to your Customs POA, this article is intended to give importers (and prospective importers) 5 simple things to think about:

"For instance, most of these boilerplate terms & conditions limit the importer's recovery for loss to $50 per shipment."

1) **Form** – If you have no idea what a Customs POA form should look like, go to the U.S. Customs and Border Protection (CBP) website, CBP.gov, and search for Document 5291. Doc. 5291 is a sample Customs POA provided by CBP. The text for the sample POA is also contained in 19 CFR § 141.32. Doc. 5291 is a good starting place, but you should definitely add to this document.

2) **Nonresident** – If the importer is a nonresident, there are more requirements than if the importer is a resident. Before signing a POA, you should investigate these requirements. For instance, a nonresident must include language in its POA authorizing its broker to accept service of process on its behalf. Similarly, the nonresident corporation must provide proof that the person signing the POA on behalf of the nonresident has the authority to do so.

3) **Ports** – A Customs POA must state the specific ports where Customs business is to be transacted on behalf of the importer. If that is all ports, then the POA must state this.

4) **Who Signs?** – The person signing on behalf of the company granting the POA must be an officer of the company (or otherwise have authority to bind the company).

5) **Terms and Conditions** – Lastly, your Customs broker will likely offer to provide the POA form to you. If this is the case, there are likely to be terms & conditions on the reverse side of the POA, or on a separate page. It is very important that you review these terms & conditions before signing. For instance, most of these boilerplate terms & conditions limit the importer's recovery for loss to $50 per shipment. So, if the broker makes a mistake, and you are penalized by CBP, there is a chance you will be left holding the bag.

While this isn't an all-inclusive checklist of items to consider when drafting or revising your Customs POA, it should get you thinking about some often over-looked items. Remember, when it comes to Customs business, the penalties can be devastating. As such, the risk will always outweigh the reward. Maximize your profits by minimizing your risk, and start with a review of your Customs POA!

For more information, please contact Thomas Kern at tkern@beneschlaw.com or 614.223.9369.

"Control What You Can Control" to Protect Your Transportation and Logistics Business and Personal Assets from Attack

As a young person easily frustrated and the oldest in a family of five children, my father would admonish my frequent "I'm not getting my way" temper tantrums with a simple phrase: "Control what you can control." I think it was my father's way of telling me not to "sweat the small stuff." Now, as a father of three, I find myself sharing that same advice with my oldest daughter. Interestingly, there is a lot more in my father's simple advice than not worrying about insignificant, trivial disputes with siblings. In fact, it can also be understood to mean that the proper attention to details (the things we can control) can be crucially important at times we might not immediately foresee.

If you are operating a business of any size, chances are good that one day you will have deal with an attempt to pierce the corporate veil of your company in litigation. As a corporation or limited liability company, the shareholders or members enjoy limited statutory protection from personal liability for the debts of the company. In litigation, a disgruntled creditor or tort claimant may seek to "pierce" that liability protection, and by doing so, make the shareholders or members personally responsible financially for the debt or claim.

This is particularly germane to the transportation and logistics industry, where plaintiffs recovering substantial verdicts will routinely seek to pierce the corporate veils of trucking/logistics companies to pursue the assets of those companies' shareholders or members. In many instances, when trucking or logistics companies are small, or start small and grow quickly, more focus is placed on meeting customer demands and growing the bottom line (and rightly so) than observing statutory corporate formalities. However, the prudent practice is to give appropriate attention to your business's structure and corporate nature, rather than avoiding or downplaying it, or suitably delegating those details to a C-level executive, accountant or attorney to protect your business from a crippling attack.

"As attorneys and courts identify more frequent and creative means to pierce the corporate veils of corporations and limited liability companies, you should take steps to protect yourself and your business from a successful corporate veil-piercing claim by methodically 'controlling what you can control.'"

Unfortunately, there is no way to prevent a person or company from *attempting* to pierce the corporate veil in order to get at the assets of a shareholder or member. More than 20 years ago, a commentator noted that "[p]iercing the corporate veil is the most litigated issue in corporate law. . . ."[1] Sadly, commentators are increasingly predicting that courts will grant veil-piercing relief in more frequent and creative ways. One study claims that "veil-piercing plaintiffs are successful in forty percent of reported cases."[2] In spite of the gloomy forecast, it is well-accepted that piercing the corporate veil remains the exception, not the rule.[3]

The test for piercing the corporate veil is substantially similar in every state (although, of course, there are nuances, like in Louisiana). For the most part, courts analyze whether:

(1) The corporation was adequately capitalized for the corporate undertaking.

(2) The corporation was solvent.

(3) Dividends were paid, corporate records were kept, officers and directors functioned properly, and other corporate formalities were observed.

(4) The dominant shareholder siphoned corporate funds.

(5) In general, the corporation simply functioned as a facade for the dominant shareholder.[4]

No single factor is determinative. Some combination of factors is required, along with some evidence of fraud, something in the nature of a sham, or some proof of using the corporate existing to perpetuate a harm against the claimant.

As attorneys and courts identify more frequent and creative means to pierce the corporate veils of corporations and limited liability companies, you should take steps to protect yourself and your business from a successful corporate veil-piercing claim by methodically "controlling what you can control." Among other things: keep the business solvent and adequately capitalized; maintain proper corporate records; refrain from entering into transactions with a shareholder, member or corporate affiliate that make absolutely no economic sense; avoid runaway intercompany debt, maintain and record corporate formalities such as annual shareholder meetings, formal board meetings and authorization for corporate transactions; do not commingle corporate funds with shareholder funds; and record, in writing, all transactions between affiliated companies and between a business and its shareholders. In short, operate your

business in such a manner as to be able, if necessary, to demonstrate separateness between affiliated entities, entities and shareholders, or both. At the end of the day, close attention to details can be your best evidence and best defense.

For more information, please contact J. Allen Jones at ajones@beneschlaw.com or 614.223.9323.

[1] John A. Swain and Edwin E. Aguilar, PIERCING THE VEIL TO ASSERT PERSONAL JURISDICTION OVER CORPORATION AFFILIATES: AN EMPIRICAL STUDY OF THE CANNON DOCTRINE, 84 B.U. L. Rev. 445, 446 (2004).

[2] Sandra K. Miller, PIERCING THE CORPORATE VEIL AMONG AFFILIATED COMPANIES IN THE EUROPEAN COMMUNITY AND IN THE U.S.: A COMPARATIVE ANALYSIS OF U.S., GERMAN, AND U.K. VEIL-PIERCING APPROACHES, 36 Am. Bus. L.J. 73, 81 (1998).

[3] 84 B.U. L. Rev. at 446, *supra* (citing, Phillip I. Blumberg, The Law of Corporate Groups: Tort, Contract, and Other Common Law Problems in the Substantive Law of Parent and Subsidiary Corporations § 6.01, at 106 (1987). *See also Advanced Tel. Sys. v. Com-Net Prof'l Mobile Radio, LLC*, 846 A.2d 1264, 1278 (2002) ("There is a strong presumption in Pennsylvania against piercing the corporate veil."); *Brown v. GE Capital Corp. (In re Foxmeyer Corp.)*, 290 B.R. 229, 237 (2003) (*citing, Harco National Insurance Co. v. Green Farms, Inc.*, 1989 WL 110537 at 5 (Del. Ch. 1989) ("Persuading a Delaware court to disregard the corporate entity is a difficult task.")).

[4] *See id.*

Recent Events

Driverless Car Summit 2013
Association for Unmanned Vehicle Systems International
Thomas Kern
June 11–12, 2013 | Detroit, MI

The State of Manufacturing & Logistics: The Road to Recovery: Chartering a New Route
Conexus Indiana and the Indianapolis Business Journal
Stephanie Penninger
June 14, 2013 | Indianapolis, IN

Conference of Freight Counsel, Semi-Annual Meeting
Eric Zalud
June 15–17, 2013 | Washington, DC

International Warehousing Logistics Association's Legal Symposium
Marc Blubaugh presented *Caution Ahead! Top Ten Transportation Topics of 2013*.
June 20, 2013 | Chicago, IL

American Trucking Association's General Counsel's Forum
Rich Plewacki attended and **Marc Blubaugh** presented *Freight Transportation Contracting Tips: The Evolution of Freight Claims in the Multimodal System*.
July 14–17, 2013 | Coeur d'Alene, ID

Transportation Lawyers Association, Summer Executive Committee Meeting
Marc Blubaugh and **Eric Zalud**
July 26–27, 2013 | Detroit, MI

National Tank Truck Carriers' Summer Membership and Board of Directors Meeting
J. Allen Jones
August 1–3, 2013 | Banff Springs, Alberta, Canada

Columbus Importers & Brokers Association, 3rd Quarter Meeting
Challenges Facing Container Deliveries
Thomas Kern
August 7, 2013 | Columbus, OH

Oregon Trucking Association Annual Convention
Martha Payne
August 23–24, 2013 | Redmond, OR

On the Horizon

Truckload Carriers Association's Independent Contractor Division Annual Meeting
Rich Plewacki
September 5, 2013 | Chicago, IL

International Warehouse Logistics Association's Annual Safety Conference
Transportation Law Update
Marc S. Blubaugh will be presenting.
September 12, 2013 | Fort Worth, TX

How to Handle Rejection: When a Consignee Says "No" to Cargo
Transportation Lawyers Association Webinar Series
Marc Blubaugh will be moderating.
September 12, 2013 | Webinar

2013 Canadian Transportation Lawyers Association Annual Conference
Martha Payne will be attending and **Eric Zalud** will be presenting on *Ethical Conflicts that Arise in a Transportation Practice*.
September 19–22, 2013 | Quebec City, Canada

Arkansas Trucking Seminar
J. Allen Jones
September 25–27, 2013 | Rogers, AK

TerraLex Annual Conference
Eric Zalud
September 25–28, 2013 | Paris, France

International Warehousing Logistics Association's "Essentials" Course
Marc Blubaugh will be presenting *Fundamentals of Transportation Law: What Warehousemen Need To Know!*
October 3, 2013 | Adelphia, MD

Innovation and Transportation Conference
Eric Zalud
October 8, 2013 | Toronto, Ontario

American Trucking Associations' Annual Management Conference & Exhibition
Marc Blubaugh and **Rich Plewacki**
October 19–22, 2013 | Orlando, FL

Transportation Lawyers Association's Transportation Law Institute
Marc Blubaugh, **Martha Payne** and **Stephanie Penninger** will be attending. **Eric Zalud** will be presenting on *Legal Aspects of Technology in the Transportation and Logistics Industry*.
November 8, 2013 | Los Angeles, CA

Transportation Lawyers Association's Executive Committee Meeting
Marc Blubaugh and **Eric Zalud**
November 9, 2013 | Los Angeles, CA

Trucking Industry Defense Association Annual Convention
Eric Zalud
November 13–15, 2013 | Orlando, FL

PE Investing in Transportation, Distribution & Logistics Companies
Capital Roundtable Conference
James M. Hill, Eric Zalud, Marc Blubaugh and **Peter Shelton**
December 5, 2013 | New York, NY

For further information and registration, please contact Megan Pajakowski, Client Services Manager, at mpajakowski@beneschlaw.com or (216) 363-4639.

Help us do our part in protecting the environment.

If you would like to receive future issues of this newsletter electronically, please email Sam Daher at sdaher@beneschlaw.com.

For more information about the Transportation & Logistics Group, please contact one of the following:

Eric Zalud, *Chair* | (216) 363-4178
ezalud@beneschlaw.com

Michael J. Barrie | (302) 442-7068
mbarrie@beneschlaw.com

Marc Blubaugh | (614) 223-9382
mblubaugh@beneschlaw.com

Matthew Gurbach | (216) 363-4413
mgurbach@beneschlaw.com

James Hill | (216) 363-4444
jhill@beneschlaw.com

J. Allen Jones III | (614) 223-9323
ajones@beneschlaw.com

Thomas Kern | (614) 223-9369
tkern@beneschlaw.com

Peter Kirsanow | (216) 363-4481
pkirsanow@beneschlaw.com

Andi Metzel | (317) 685-6159
ametzel@beneschlaw.com

Lianzhong Pan | (011-8621) 3222-0388
lpan@beneschlaw.com

Martha Payne | (541) 764-2859
mpayne@beneschlaw.com

Stephanie Penninger | (317) 685-6188
spenninger@beneschlaw.com

Rich Plewacki | (216) 363-4159
rplewacki@beneschlaw.com

Teresa Purtiman | (614) 223-9380
tpurtiman@beneschlaw.com

Peter Shelton | (216) 363-4169
pshelton@beneschlaw.com

Sarah Stafford | (302) 442-7007
sstafford@beneschlaw.com

Katie Tesner | (614) 223-9359
ktesner@beneschlaw.com

E. Mark Young | (216) 363-4518
myoung@beneschlaw.com

Pass this copy of *InterConnect* on to a colleague, or email Adriane DeFiore at adefiore@beneschlaw.com to add someone to the mailing list.

Printed on recycled paper.

Benesch
Attorneys at Law