MAYER·BROWN

Issue 19 | Summer 2013

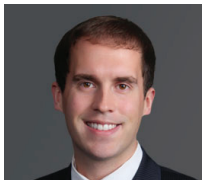
Business & Technology Sourcing
REVIEW

About Our Practice

Mayer Brown's Business & Technology Sourcing (BTS) practice is one of the global industry leaders for Business Process and IT Outsourcing as ranked by Chambers & Partners, The Legal500 and the International Association of Outsourcing Professionals (IAOP). With more than 30 dedicated lawyers—many having previous experience with leading outsourcing providers and technology companies—the practice has advised on nearly 300 transactions worldwide with a total value of more than $100 billion.

Editors' Note

Kevin A. Rang
Chicago
+1 312 701 8798
krang@mayerbrown.com



David J. Messerschmitt
Washington, DC
+1 202 263 3161
dmesserschmitt@
mayerbrown.com

Lei Shen
Chicago
+1 312 701 8852
lshen@mayerbrown.com

Welcome to the Summer 2013 edition of the Mayer Brown *Business & Technology Sourcing Review*.

Our goal is to bring you smart, practical solutions to your complex sourcing matters in information technology and business processes. We monitor the sourcing and technology market on an ongoing basis, and this Review is our way of keeping you informed about trends that will affect your sourcing strategies today and tomorrow.

In this issue, we cover a range of topics, including:

- Delivering Value in Finance and Accounting Outsourcing
- Limitations on Liability Exceptions for Gross Negligence and Willful Misconduct and the Implications for Outsourcing Agreements
- Letters of Intent and Other Preliminary Agreements
- Governance: Practical Steps to Making It Work
- Mobile Application Privacy: An Overview of the Recommendations from the FTC and the California Attorney General
- The 2013 Cybersecurity Executive Order: Potential Impacts on the Private Sector
- Cyber Security Program Highlights

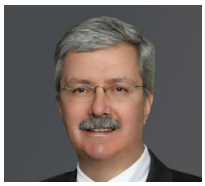
You can depend on Mayer Brown to address your sourcing matters with our global platform. We have served prominent clients in a range of sourcing and technology arrangements across multiple jurisdictions for over a decade.

We'd like to hear from you. If you have any suggestions for future articles or comments on our current compilation or if you would like to receive a printed version, please email us at BTS@mayerbrown.com.

If you would like to contact any of the authors featured in this publication with questions or comments, we welcome your interest to reach out to them directly. If you are not currently on our mailing list, or would like a colleague to receive this publication, please email contact.edits@mayerbrown.com with full details. ◆

Delivering Value in Finance and Accounting Outsourcing

Daniel A. Masur
Brad L. Peterson
Derek J. Schaffner



Daniel A. Masur
Washington, DC
+1 202 263 3226
dmasur@mayerbrown.com

Brad L. Peterson
Chicago
+1 312 701 8568
bpeterson@mayerbrown.com

Derek J. Schaffner
Washington,. DC
+1 202 263 3732
dschaffner@mayerbrown.com

Introduction

Finance and accounting ("F&A") functions were among the first business processes to be outsourced, and F&A remains one of the most robust outsourcing areas for business today. The most commonly outsourced F&A functions have included the order-to-cash, procure-to-pay and order-to-report cycles, payroll and travel and expense ("T&E") processing, and similarly transactional functions. However there is momentum to outsource more strategic activities, such as budgeting, internal auditing and strategic sourcing. Across this spectrum, customers can use contractual mechanisms to help secure commitments to deliver the anticipated value from the outsourcing project. This article will share some key insights and lessons that we have learned from handling dozens of F&A deals, including some of the largest ever attempted.

The Value of Contract Terms

Contract terms can deliver value to F&A customers in three ways. First, contract terms can secure commitments to perform the F&A functions for a reasonably firm price in accordance with a customer's business requirements and contracts, as well as with applicable laws.

Commitments deliver value by providing an assurance of the needed services and by delivering anticipated savings. Second, contract terms can provide options to increase, reduce or change volumes and requirements; these options deliver value if there is a change during the term. Finally, contract terms can provide a financial incentive for a provider to perform in a way that increases the value of the customer enterprise, even in areas where there is no express contractual commitment. These financial incentives deliver value in the same way that paying a commission to a sales representative delivers value: by motivating the provider to use its influence in areas that it cannot control. For example, a provider might commit to an incentive arrangement around invoice processing speed or reductions in days' sales outstanding.

The Spectrum of F&A Outsourcing

Providers offer a spectrum of solutions for outsourcing F&A functions. One end of the spectrum focuses on the performance of non-discretionary tasks, often for less money than it costs the customer to perform those tasks. These cost savings are largely achieved via labor arbitrage, centralization in shared delivery centers and tool consolidation. Obvious customers for these types of services are large organizations that have invested

heavily in accounting systems that are not candidates for retirement or replacement. On the other end of the spectrum, some providers offer turn-key F&A solutions that often leverage Software-as-a-Service ("SaaS") platforms with cloud capabilities. These solutions can be very attractive to small- and medium-sized organizations because this plug and play approach may offer more robust capabilities than the current in-house solution. These solutions are also increasingly attractive to large organizations for functions such a payroll processing.

Each end of this spectrum presents different legal and contractual challenges, options and trade-offs. This article focuses on the larger outsourcing transactions where the provider is taking over an existing function using customer systems. We would note, though, that at the other end of the spectrum customers need to watch for the issues generally seen in cloud and SaaS agreements.

Securing the Services Commitment

So, how can the outsourcing agreement be leveraged to secure commitments for F&A outsourcing? Sourced services are typically defined by accounting processes and financial systems, although the scope may differ by geography or business unit (for example, different systems or different business practices). You can add further clarity and commitment by describing the steps in the accounting process, including the systems utilized and handoffs between customer and provider. Carefully defining the handoff points not only help to avoid fumbled handoffs but also helps to maintain control and measure performance. For example, if a customer outsources a portion of the accounts payable process, service levels can be defined for the outsourced portion to reinforce performance management and align the provider's incentives with the customer's needs.

The handoff points also play an important role to ensure that control objectives are met. A customer may decide not to outsource all accounts payable functions and, instead, retain control of certain critical pieces. For example, a customer may retain the processing and payment of invoices to certain critical suppliers to ensure that missed payments do not result in raw material interruptions. While a service level could be used in lieu of retaining this function internally, the cost of raw material interruptions may be greater than any service level credit.

Compliance failures are a primary risk in F&A outsourcing arrangements. This often involves a trade-off between maintaining the internal controls relied upon by the customer for F&A functions generally and leveraging the internal controls that the provider has designed and implemented in its shared service delivery centers. Requiring the provider to comply with customer-defined internal controls may prevent the provider from leveraging the reliability, efficiency and cost savings designed into its multi-customer service delivery model without offering greater compliance assurances or other value.

Therefore, it is recommended that the customer start with high-level F&A control objectives and ask the provider to propose internal controls that will meet those objectives. If the proposed controls are acceptable, they should be memorialized in the service management and governance manual or desk procedures. Under this approach, the provider will still need to comply with those controls, but those controls can be upda ted more quickly to address new threats.

The outsourcing agreement must contain a robust set of audit rights that include not only internal audit rights, but also audits by government regulators and other third parties.

Audits

Audit rights are an important element of any outsourcing deal, but they take on more significance when the scope includes F&A functions. The outsourcing agreement must contain a robust set of audit rights that include not only internal audit rights, but also audits by government regulators and other third parties. For F&A arrangements, there are typically two types of audits: (1) audits to confirm whether the provider is meeting its contractual commitments and (2) audits related to the F&A functions themselves. These latter audits can be thought of as the same audits that the customer would need to perform on the F&A functions if those functions were performed in-house. The scope of such audits is more focused on whether or not the outsourced F&A functions are performed in accordance with GAAP and the cus-

tomer's accounting policies than whether the provider is doing what it agreed to do. Regardless of the type of audit, however, providers may seek to limit the amount of audit support that is included in the base charges. In that case, the customer should try to build in a certain amount of audit support at a fixed price with the option of purchasing additional audit support if necessary. However, there should be an exception for audits resulting from the provider's breach of its obligations.

Because of the importance of maintaining strong controls over the performance of F&A functions, it is also important that the agreement contain a commitment by the provider to have its operations audited under SSAE 16 or ISAE 3402 (the successors to SAS 70) and to deliver an unqualified controls audit report. To provide a stronger incentive for the provider to deliver an unqualified controls audit report, the agreement should contain financial credits, enhanced liability and/or termination rights for the failure to provide an unqualified controls audit report. While most providers of F&A services will perform a controls audit once per year, this audit is typically limited to controls in the provider's shared delivery center. Because the provider's controls audit report is generally not customer-specific, each customer must separately contract with either the provider or the customer's auditor to audit the customer-specific controls.

Pricing

Customers generally seek a secure commitment to savings and, as a result, prefer either fixed prices or prices based on such outputs as invoices processed or employees paid. Fixed prices are common on transition activities because the provider generally has a deep understanding of the effort involved to move from the customer's current environment to the provider's solution. Likewise, transformation and governance activities are generally within a provider's control and area of historical knowledge and are commonly performed for a fixed price. Making those fixed prices for transition and transformation activities be subject to deliverable credits for missed milestones can provide a valuable incentive for achieving those milestones. Similarly, a fixed price approach is often used for the cost of tools and technology used to support and deliver the services because the provider generally understands the costs associated with these items better than the customer does.

Customers generally seek a secure commitment to savings and, as a result, prefer either fixed prices or prices based on such outputs as invoices processed or employees paid.

F&A deal pricing is often more complicated for the actual performance of F&A functions. Transaction-based pricing is fairly common in IT deals, but there is more variability in F&A solutions, and F&A tasks are frequently measured in ways that do not lend themselves to transaction-based pricing. For example, a customer may track the number of invoices that it processes but not how many of those invoices require manual intervention or the extent of intervention needed. Thus, the parties may be uncomfortable with a "price per invoice" unless they know the number of invoices requiring manual intervention.

As a result, the parties often default to full-time equivalent ("FTE") pricing models as it is easier to measure and price the labor effort associated with a basket of F&A activities than the individual tasks. This assures the provider its profitability, but often means that the customer bears the risk that the provider will over-hire, be inefficient or fail to deliver true full-time effort from its people.

FTE-based pricing models are often viewed as lacking any meaningful commitments to savings and cost improvements.

However, this does not need to be true. One contractual approach to achieving savings commitments under an FTE-based model involves the creation of an "FTE glide path" that starts at the current number of FTEs and then declines based on the provider's committed productivity improvements. The outsourcing agreement can contain a mechanism to adjust the glide path based on volume and provide that the fees charged to the customer will be based on the lesser of the actual number of FTEs used to deliver the services or the FTE glide path. To incentivize the provider to achieve additional productivity gains beyond those assumed in the FTE glide path, a gain-sharing

structure can share some of the savings if the number of actual FTEs is less than the FTE glide path.

Ideally, the FTE-based customer has an option to replace FTE-based pricing with a transaction-based approach. As discussed above, the parties often lack adequate data to incorporate transaction-based pricing at the time of contracting. To gain the value of transaction-based pricing without the data to support it at signing, the agreement should contain options that allow the conversion from an FTE-based model to a transactional one. To do so, the parties must first agree on the "resource units" being measured, such as "invoices processed." For F&A deals, the term "transaction volume unit" ("TVU") is often used in lieu of the more IT-centric "resource unit." Once the TVU is defined, the provider should measure and report on monthly actual TVU consumption. Additionally, the provider should measure and report on the number of FTEs required to process the given TVU volume. After enough TVU data has been collected to determine a per-TVU price, the agreement should contain an option that allows the customer to convert to this alternative method.

Another important issue is the allocation of currency fluctuation risk and wage inflation risk. If the provider is performing the outsourced functions from another country, the provider is typically being paid in one currency (such as Dollars or Euros) and incurring some or all of its performance costs in a different currency (such as Rupees). Currency fluctuations thus may change the relationship between the charges to the customer and the provider's cost, and some providers ask the customer to bear that risk. Additionally, wage inflation in some offshore locations, such as India, has historically been far greater than wage inflation in the United States, Europe and other countries.

Most customers are uncomfortable with the risk of unchecked currency fluctuation or wage inflation based on an offshore standard, especially since they have no control or ability to mitigate the risk. These risks can be shared with a variety of mechanisms, including price adjustments tied to an appropriate COLA index in the customer's home country or currency exchange rates and perhaps allocation percentages, thresholds, caps and collars.

Key Options for Retaining Leverage and Managing Change

Mechanisms for retaining control of outsourced functions and managing change are critical in F&A outsourcing because of the high degree of uncertainty during the initial stages of the relationship (e.g., FTE-based pricing, productivity commitments). Nonetheless, there are certain options that should be included in the agreement that the customer can exercise to retain leverage in the relationship.

Mechanisms for retaining control of outsourced functions and managing change are critical in F&A outsourcing because of the high degree of uncertainty during the initial stages of the relationship.

The option to award (or deny) new services to the provider can be a powerful incentive to make customer satisfaction is a top priority for the provider. Likewise, the option to in-source or move work to third parties for existing services gives the customer the opportunity to fix problems in the event the provider cannot perform the services as expected. For example, if the provider cannot process invoices in a particular language, the customer needs the ability to move that work to a third party that can perform those services. Moreover, the right to move work away from the provider can be important in addressing other contract issues and disputes.

Another powerful contractual tool is the option to withhold disputed charges, including a commitment by the provider to continue to provide the services regardless of the level of disputed charges. Short-paid invoices quickly garner the attention of provider senior management, which, in turn, focuses attention on the underlying problem causing the dispute.

Termination rights are valuable options and can be valuable incentives. Termination rights commonly may be exercised "for cause" upon a material breach by the provider and do not require the payment of termination charges. Additionally, the customer should have the option to terminate "for convenience" or upon a change of provider control with termination charges. Regardless of the type of termination, the

agreement should include the option for the customer to continue receiving the steady-state services during the disengagement period for a predetermined price that avoids price gouging. Other options to consider under termination include the ability to hire provider personnel for service continuity and knowledge transfer purposes and the ability to obtain rights to third-party software, equipment and materials to the extent necessary to transition the services in-house or to a new provider.

Key Contract Clauses for Provider and Third-Party Technology

The F&A outsourcing model continues to evolve. At one point, the primary driver was labor arbitrage based on lower FTE costs offshore. However, wage differentials are shrinking. The focus today is more on tools that reduce costs and increase speed and accuracy of the F&A functions. Each provider touts its own tools, and many use third-party products.

Such tools present a challenge from a contractual perspective because the customer would like a commitment from the provider that the tools will deliver the promised value. Options such as the ability to terminate transition if the tools are not working as promised can mitigate that risk. Also, customers are seeking corresponding reductions in transaction pricing or maximum FTEs to offset costs for new tools.

Often, the parties must build interfaces between provider tools and customer systems. The allocation of operational and financial responsibility for developing those interfaces should be clearly documented in the agreement. Likewise, the agreement should define stage gates (including specifications and acceptance criteria) for moving the integrated system into the production. If the provider is relying on third-party tools to perform some of the services, the obligation to obtain necessary required consents should be documented in the agreement, as well as an option for the customer to work directly with the third party.

Provisions commonly sought by customers in SaaS and license agreements can help them mitigate the risks and secure the value of these tools. Also, customers may consider licensing or subscribing to third-party tools directly from the third party to allow continuity in a termination and the ability to use the same tools across their enterprises.

Compliance with Applicable Laws

Compliance with laws is a challenging topic in F&A outsourcing because of the range of compliance obligations and the differing ways that different customers and suppliers allocate responsibility for F&A functions. Laws that require compliance can be grouped into at least four categories: (1) laws directly impacted by the outsourced functions, such as data privacy and export control laws; (2) industry-specific laws, such as licensing requirements for third-party pension administrators; (3) laws specific to the F&A functions being performed, such as payroll tax laws, ACH rules and debt collection restrictions; and (4) generally accepted accounting principles and customer policies that, if not followed, may result in a misstatement of financial results in violation of laws.

Instead of taking a cookie-cutter approach to compliance with laws, the parties can consider which party will be better able to monitor changes to which laws and enforce compliance of which laws in the applicable jurisdictions. For example, most providers have created shared delivery centers to achieve a particular set of results, which may involve compliance with such common functions as applying proper taxes to payroll. Part of the cost savings the customer will receive as a result of outsourcing certain F&A functions is based on leveraging those shared delivery centers. On the other hand, some compliance functions are better handled by modifying the customer's accounting systems. With that approach, the customer can retain the right to define its requirements and ask the provider to define what it can do to meet those requirements.

Final Thoughts

Finance and accounting outsourcing involves unique opportunities and risks because of the central, highly regulated role of the F&A function within an organization. The right contract terms can help to maximize value and avoid costly pitfalls by securing commitments, providing options and aligning incentives. You can get the right terms by combining standard outsourcing provisions with unique terms designed for the unique challenges of F&A outsourcing. ◆

Limitations on Liability Exceptions for Gross Negligence and Willful Misconduct and the Implications for Outsourcing Agreements

Danielle K. Fisher
Linda L. Rhodes

Danielle K. Fisher
Washington, DC
+1 202 263 3338
dfisher@mayerbrown.com

Linda L. Rhodes
Washington, DC
+1 202 263 3382
lrhodes@mayerbrown.com

In outsourcing agreements, parties typically limit their liability to each other. The parties often exclude from those limitations on liability damages caused by gross negligence or willful misconduct. The definitions of gross negligence and willful misconduct vary by state and the conduct that courts consider as falling under those definitions depends on the facts of each case. This article examines the definitions of gross negligence and willful misconduct, the difficulty in demonstrating to courts that a party's conduct meets the standards imposed by those definitions and the implications for outsourcing agreements. For purposes of this article, we focus on New York law, commonly selected as the governing law in large outsourcing transactions.

The definitions of gross negligence and willful misconduct vary by state and the conduct that courts consider as falling under those definitions depends on the facts of each case.

Limitation of Liability Provisions

Outsourcing agreements typically prohibit each party from being held liable for any incidental, consequential, punitive, special or other indirect damages. In addition, these agreements typically place a cap on the total amount of damages for which either party can be liable in connection with the agreement. The result is to disallow a party from recovering the full damages caused by the actions of the other party. While such an allocation of risk may be acceptable in the case of an ordinary breach of contract by the other party, the allocation of risk is not typically considered acceptable when damages result from egregious action on the part of the other party or where the stakes of nonperformance by the other party are so high that appropriate incentives need to be put in place to ensure that the other party fulfills its obligations under the agreement.

In such cases, the parties usually want the right to recover special, consequential and incidental damages and damages in an amount greater than the liability cap. Examples of exclusions from limitations of liability include losses resulting from a breach of confidentiality, refusal to provide services, death, bodily injury, damage to tangible property, violation of applicable law, gross negligence or willful misconduct.

While certain of the above exceptions may be proved relatively easily, proving that a party's conduct constitutes gross negligence or willful misconduct is often more difficult. By understanding the definitions under the laws of the state governing the agreement and

the courts' decisions on what conduct falls under the definitions, customers can better understand their rights and risks and the implications for a particular outsourcing agreement.

By understanding the definitions under the laws of the state governing the agreement and the courts' decisions on what conduct falls under the definitions, customers can better understand their rights and risks and the implications for a particular outsourcing agreement.

Enforcement of Limitation of Liability Provisions

With certain exceptions, courts enforce express agreements between parties that limit damages to be recovered in the event of a breach of contract.[1] Parties are free to "bargain against liability for harm caused by their ordinary negligence in performance of contractual duty."[2] Nevertheless, courts will not enforce an exemption from liability if it applies to "harm willfully inflicted or caused by gross or wanton negligence."[3]

New York courts generally enforce limitation of liability provisions since such provisions represent "the parties' Agreement on the allocation of the risk of economic loss in the event that the contemplated transaction is not fully executed."[4] However, even when parties limit liability but do not specifically exclude damages caused by willful misconduct or gross negligence, New York courts will not enforce the provision if the "misconduct for which it would grant immunity smacks of intentional wrongdoing"[5] or if the provision will insulate a party from damages caused by its own grossly negligent conduct.[6] Nevertheless, a party trying to overcome a limitation of liability provision by claiming that the other party engaged in willful misconduct or gross negligence must meet the standards described below.

What Are the Standards for Gross Negligence and Willful Misconduct?

The standards for proving gross negligence and willful misconduct are high.

Gross Negligence. Under New York law, misconduct that rises to the level of gross negligence must show "reckless indifference to the rights of others."[7] The conduct must show a "failure to use even slight care or conduct that is so careless as to show complete disregard for the rights and safety of others."[8] The gross negligence standard focuses on the severity of a party's deviation from reasonable care.

Willful Misconduct. In New York, willful misconduct occurs when a "person intentionally acts or fails to act knowing that (his, her) conduct will probably result in injury or damage."[9] Willful misconduct can also occur when "a person acts in so reckless a manner or fails to act in circumstances where an act is clearly required, so as to indicate disregard of (his, her) action or inaction."[10] A party claiming willful misconduct must show an "intentional act of unreasonable character performed in disregard of a known or obvious risk so great as to make it highly probable that harm would result."[11] The willful misconduct standard is similar to the gross negligence standard; however, it focuses more on the harm that a party's action or inaction caused.

What Conduct Meets the Standards of Gross Negligence and Willful Misconduct?

What conduct do New York courts consider as meeting the standards for gross negligence or willful misconduct? The determination depends highly on the facts of each case. The following cases provide some insight into the decisions of New York courts making this determination.

In one case, a computer software developer licensed its base software to the customer and was under an obligation to provide enhancements thereto.[12] The customer rejected two sets of enhancements provided by the developer and a fee dispute arose, after which the developer discontinued performance under the agreement. Under the agreement's limitation of liability clause, the developer was absolved from any liability for certain indirect damages. There was an exception to the limitation of liability for, among other things, damages arising out of the developer's willful acts or gross negligence. The court found that parties to the agreement did not intend for the developer's discontinuation of services to constitute a willful act or gross negligence and, therefore, upheld a decision to enforce the limitation of liability clause.

In another case, an airline entered into an agreement for the installation of infrastructure for in-flight Internet service.[13] The airline alleged that, with the encouragement of the Internet service provider, it invested millions of dollars in installing the Internet service infrastructure while the service provider secretly considered terminating the in-flight Internet service. The service provider ultimately decided to terminate the service. The airline claimed that the service provider's actions constituted gross negligence and that, therefore, the contractual limitations on liability should not apply. The court found that the service provider's conduct did not meet the "reckless disregard" standard required to prove gross negligence and, accordingly, upheld the contract's limitation on liability provisions.

If a customer wants to ensure that a specific type of misconduct by a service provider falls outside of the limitation of liability clause, the customer should specifically describe such misconduct in the outsourcing services agreement.

A New York court found that a home inspector's failure to identify problems in a house constituted gross negligence in another case.[14] The services agreement limited the home inspector's liability for any consequential, exemplary or incidental damages in the event of a breach or negligent inspection; however, the limitation did not apply to any grossly negligent conduct or willful misconduct. The home inspector failed to identify hazardous conditions during the inspection that endangered the lives of the homeowners. The court determined that the home inspector's conduct showed a complete disregard for the safety of the homeowners and, thus, the homeowners were entitled to obtain damages outside of the limitation.

Implications for Outsourcing Agreements

Customers need to carefully consider the exceptions to the limitations on liability included in their outsourcing agreements. Although state law may imply an exception for gross negligence or willful misconduct, losses arising from such conduct should be an express exception to the limitations on liability in the outsourcing agreement in order to avoid the need to establish the public policy exception and research the issue under each state law. Moreover, a customer needs to consider how difficult and costly it will be to prove to a judge or jury that a service provider's conduct meets the high standards required to establish gross negligence or willful misconduct.

If a customer wants to ensure that a specific type of misconduct by a service provider falls outside of the limitation of liability clause, the customer should specifically describe such misconduct in the outsourcing services agreement. In two of the cases described above, excluding the service provider's refusal to provide services from the limitation of liability would have provided a clearer standard for the customer to prove. Since the limitation of liability provision has a significant impact on the allocation of risk between parties to an outsourcing agreement, customers should ensure that any specific losses or misconduct that should not be subject to contractual limitations on liability are clearly and sufficiently identified as exclusions to the limitation of liability provisions. ◆

Endnotes

1 5 Corbin on Contracts § 1068 (1964).

2 6A Corbin on Contracts § 1472 (1962).

3 *Id.*

4 See *Metropolitan Life Ins. Co. v. Noble Lowndes Int'l*, 643 N.E.2d 504, 507 (N.Y. 1994).

5 See *Kalisch-Jarcho, Inc. v. New York*, 448 N.E.2d 413, 416 (N.Y. 1983).

6 See *id.*

7 See *id.*

8 See *Johnson v. Smith*, 2006 N.Y. Misc. LEXIS 2618 at **37-38 (City Ct. of N.Y. (Jefferson County) Sept. 8, 2006).

9 See *id.* at *3 (quoting New York Pattern Jury Instructions § 2.10A).

10 See *id.* at *3 (quoting New York Pattern Jury Instructions § 2.10A).

11 See *McDuffie v. Watkins Glen Int'l, Inc.*, 833. F. Supp. 197, 203 (W.D.N.Y., Sept. 3, 1993).

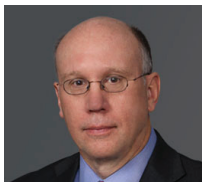
12 *Metropolitan Life Ins. Co. v. Noble Lowndes Int'l*, 643 N.E.2d 504 (NY 1994).

13 See *Deutsche Lufthansa AG v. Boeing Co.*, 2007 U.S. Dist. LEXIS 9519, 2007 WL 403301 (S.D.N.Y. Feb. 2, 2007).

14 See *Johnson v. Smith*, 2006 N.Y. Misc. LEXIS 2618 (City Court of New York (Jefferson County) Sept. 8, 2006).

Letters of Intent and Other Preliminary Agreements: *Married, Engaged or Just Friends?*

Robert J. Kriss
Gregory A. Manter



Robert J. Kriss
Chicago
+1 312 701 7165
rkriss@mayerbrown.com

Gregory A. Manter
Chicago
+1 312 701 8648
gmanter@mayerbrown.com

The Delaware Supreme Court recently decided that an agreement that the parties "will negotiate in good faith with the intention of executing a definitive License Agreement in accordance with the terms set forth in the License Agreement Terms Sheet" gave rise to an enforceable contract and a right to recover full contract damages, notwithstanding the fact that every page of the Term Sheet was labeled "Non Binding Terms." The case, *SIGA Technologies, Inc. v. Pharmathene, Inc.*, 2013 WL 2303303 (Del.Supr. May 24, 2013), creates new risks that a party might find itself committed to a transaction when it thought it had the right to walk away from the bargaining table at any time and for any reason. Letters of intent and other preliminary agreements are often used in connection with software implementation projects or information technology outsourcing relationships when the parties decide that work should begin before they have finished negotiating a definitive agreement. This article will address how a customer can avoid unintended commitments and better control the negotiating process to achieve its objectives.

The Delaware Case

SIGA Technologies Inc. ("SIGA") was engaged in developing an antiviral drug for the treatment of smallpox. SIGA required additional financing to continue its project and turned to Pharmathene, Inc. ("Pharmathene") for funding. Initially, the parties contemplated structuring the capital infusion in the form of a technology license. A license agreement term sheet (LATS) was negotiated that included most of the economic terms of the deal. Each page of the terms sheet was stamped with the legend "Non binding Terms." Later, the parties decided that Pharmathene would acquire SIGA in a merger. The merger agreement provided that if the merger was terminated, the parties agreed to negotiate in good faith a definitive license agreement in accordance with the terms of the LATS.

After the merger agreement was executed but before the transaction closed, SIGA started to obtain substantial funding from the federal government. As a result, SIGA was no longer interested in consummating the merger and refused to extend the closing date, thereby terminating the merger agreement. SIGA and Pharmathene then began negotiating the license agreement. Because SIGA's

financial condition had improved since the economic terms in the LATS had been negotiated, SIGA proposed substantial changes to those terms. Ultimately, the parties reached an impasse in the negotiations. Pharmathene sued SIGA to enforce the agreement to negotiate the license agreement in good faith in accordance with the original terms of the LATS.

The trial court concluded that if the parties had negotiated the open terms not included in the LATS in good faith, the parties would have reached agreement on those terms. The court also concluded that, as a matter of law, the agreement to negotiate in good faith required SIGA not to propose material changes to the economic terms that previously had been agreed upon and included in the LATS. Therefore, the trial court held that SIGA had breached the agreement to negotiate in good faith and was liable for full contract damages, including the profits Pharmathene would have realized if the license agreement had been executed according to the original economic terms in the LATS.

The court also concluded that, as a matter of law, the agreement to negotiate in good faith required SIGA not to propose material changes to the economic terms that previously had been agreed upon and included in the LATS.

The Delaware Supreme Court affirmed the trial court's decision and explained several principles of Delaware law applicable to the enforcement of preliminary agreements. First, where the parties enter into a preliminary agreement to negotiate in good faith a definitive agreement in accordance with the terms of the preliminary agreement, neither party can subsequently propose terms inconsistent with those established in the preliminary agreement. Second, the parties are not obligated to reach agreement on the terms that were not included in the preliminary agreement, and a good faith disagreement as to the open terms will preclude enforcement of a definitive agreement. Third, the court will make a factual determination as to the reasons that the parties failed to reach a definitive agreement. If the court concludes that the parties failed to reach a definitive agreement because one of the parties no longer was willing to be bound by the terms in the preliminary agreement, the court will find that party to be acting in bad faith. Finally, where the court determines that, but for the defendant's bad faith negotiations, the parties would have reached an agreement on the open terms, the plaintiff will be entitled to recover contract expectation damages, including lost profits, based upon the terms of the preliminary agreement.[1]

Contract-Drafting Lessons Learned — General Principles

- If you enter into a preliminary agreement to negotiate in good faith to reach a definitive agreement in accordance with the terms of the preliminary agreement, you ultimately may be bound by the terms of the preliminary agreement.
- Even if you do not use the term "good faith" in the preliminary agreement, you may be bound to negotiate in good faith if other language in the preliminary agreement indicates that the parties intended to enter into a final agreement and only reserved the right to resolve open issues through subsequent negotiation.
- If you want to preserve the right to terminate negotiations at any time and for any reason, then you should not agree in the preliminary agreement to negotiate in good faith, and you should expressly state that the parties have the right to terminate negotiations at any time and for any reason and not be bound by the terms of the preliminary agreement.
- Stating that the terms of a preliminary agreement are non-binding and that a definitive agreement is necessary to bind the parties may not be sufficient to avoid a duty to negotiate the definitive agreement in good faith. Again, it is safer to expressly state that the parties may terminate negotiations at any time for any reason and not be bound by the terms of the preliminary agreement.
- If you want the parties to be bound in certain respects so that work can proceed before a full,

definitive agreement is negotiated and executed, be specific about what is agreed to be done and what are the consequences of terminating the negotiations. For example, it is better to know that termination will cost "x" dollars than to have uncertainty as to whether you have agreed to negotiate the full agreement in good faith and, as a result, may be liable for full contract damages, including lost profits, if you terminate negotiations.

Application to IT System Implementations and Outsourcing Transactions

Frequently during the course of negotiations for IT system implementations and outsourcing transactions, one party — typically, the vendor — will propose to start work immediately, before the full contract is complete, through a signed preliminary agreement or letter of intent (LOI).

Examples of reasons given by vendors for executing an LOI include the following:

- The business terms are settled, so there is no need to hold up work to let the legal details catch up.
- The vendor's delivery team is ready now, and the customer risks losing the best resources if it waits for completion of the final agreement.
- To meet a customer deadline, equipment needs to be ordered now, and any delay in the start of the project will result in a day-for-day delay past the customer's deadline.
- The customer should provide some show of commitment, even if the LOI is non-binding, before the vendor makes the effort to complete the final documentation. (This is often pitched by the sales team as a plea to help alleviate pressure from the vendor's management to get the full deal signed up immediately.)

Before addressing the validity of those reasons, it is important to note that, as between the parties, any signed LOI to begin temporary work will result in a loss of leverage for the customer with an offsetting gain in leverage by the vendor for the upcoming detailed negotiations. After all, once work has begun and the vendor is entrenched within the customer organization and in the project itself, it will be very evident to both parties that there are few, if any, issues that could constitute a "deal-breaker" resulting in a stoppage of work, a loss of value for work already performed and a loss of internal reputation for the customer team that agreed to proceed. A skilled vendor will exercise its new-found leverage to maximize its revenues on a "sure deal" and minimize its risk and exposure to failure through negotiation of the final terms.

Any signed LOI to begin temporary work will result in a loss of leverage for the customer with an offsetting gain in leverage by the vendor for the upcoming detailed negotiations.

In many cases, the vendor's reasons for requiring an LOI may be illusory or simply window-dressing to maximize that leverage. Or, the vendor will present challenges that have a kernel of truth, but that can be addressed or mitigated without the parties signing an LOI. For example, a vendor's suggestion that it will pull the "A" team from the customer's account without an LOI to start temporary work could be strategic positioning only raised in order to pressure a customer. Likewise, there is rarely, if ever, a requirement in a bidding process for a customer to evidence its commitment to a vendor before finalizing the full detailed agreement.

Once a customer agrees to enter into an LOI, the vendor's initial draft will typically seek to bind the customer for the entire term of the full deal, identifying rates and pricing. While this pricing is commonly attached as an exhibit to the LOI, detailed descriptions of the services and/or the "solution" being created by an implementation—in other words, the vendor's commitments—are rarely included, on the theory that those details are "understood" well enough by the technical teams and will be captured in the final agreements. While customers are frequently successful in pushing back on the vendor to make the LOI non-binding and limit their commitment to only negotiate in good faith, they are typically not in a position to attach the detailed requirements for what they are buying. The customer is left with clear pricing but no commitment to scope or legal terms.

Setting aside the inherent losses of leverage for a customer in entering into an LOI, the recent *SIGA* ruling compounds the risks of an LOI to a customer in two ways:

- First, teams that are agreeing to a non-binding, good faith negotiation LOI typically view that LOI as a low-risk proposition that will not require or presume completion of a final deal. With that perspective, the content of an LOI is often pulled together hastily and is not given the level of review and consideration that is reserved for other signed contracts. The *SIGA* ruling places a burden on the customer, once it has signed an LOI, to complete negotiations in accordance with the LOI terms or risk a claim of bad faith negotiations. Failure to live up to the terms of the LOI could ultimately make that customer liable for the vendor's expectation damages for the full deal (including contemplated profits on the full deal) if negotiations terminate prior to execution of that deal.
- Second, per the *SIGA* ruling, after an LOI is signed, a party may be prevented from proposing terms that are inconsistent with those established in the LOI. As noted above, in LOIs, there is a focus on rates and pricing (i.e., the revenue stream for the vendor) that is favored over describing the value that the customer will receive for that pricing. As a result, a typical LOI-bound customer is like a car buyer who has committed to a price before knowing the make or model of the car or its features. If an LOI identifies clear pricing for an undefined system or project, then the *SIGA* ruling suggests that good faith negotiations must take place regarding the system or project details only, because pricing will be interpreted as having been settled already. The customer is constrained from proposing materially lower pricing as it learns more about what is excluded from the features of the system or the scope of the project, out of fear that any such proposal could be perceived as negotiating in bad faith.

In summary, for IT and outsourcing arrangements, the *SIGA* ruling makes the already-suspect contracting tool of the LOI that much more unattractive to a customer who is seeking to contract for value and sustain leverage in negotiations with a vendor.

Mitigating Risks Where an LOI Is Unavoidable

In spite of the many reasons described above for a customer to resist agreeing to an LOI with a vendor, there may be times when, for good business reasons, a customer will need a vendor to begin work on a project immediately in order to meet a business-driven or technically required deadline. Sometimes, even the loss of leverage for the remaining negotiations will be more palatable to a customer than a missed deadline. In those cases, the drafting principles identified earlier in this article will be particularly important when negotiating the LOI. Specifically, the LOI should exclude any commitment by the parties to negotiate in good faith with the intention of executing a final agreement, expressly reserve the right of each party to end negotiations for any reason and clarify that all points of the final deal (e.g., price, scope and legal terms) remain subject to further negotiation.

> [I]t is critical that the LOI account for all possible outcomes and scenarios if the LOI is terminated prior to completion of the final agreement.

Finally, it is critical that the LOI account for all possible outcomes and scenarios if the LOI is terminated prior to completion of the final agreement. This includes describing the disposition and responsibility for all critical elements of that temporary work, including the following:

- Identifying which portions of the temporary services, if any, will be billable to the customer if negotiations fail.
- Identifying who will be responsible for any ordered equipment, software or other stranded assets that cannot be returned.
- Determining whether the customer will be allowed to retain the planning documents and materials that are developed prior to cancellation of the temporary services.

Addressing these issues and other similar concerns will minimize the risk of unintended consequences flowing from a terminated LOI. Even if the LOI is not terminated, good guidelines will assist the customer in retaining some amount of leverage after signing the LOI, particularly if the terms are designed so that the vendor risks losing some portion of the revenue for the temporary services performed if the larger deal falls apart. ◆

Endnotes

1 Although this decision is based upon Delaware law, the Delaware Supreme Court relies heavily on decisions by New York state courts and federal courts construing New York law. The rules discussed above most likely will also apply to disputes governed by New York law.

Governance: Practical Steps to Making it Work

Peter Dickinson
Megan Paul

Peter Dickinson
London
+44 20 3130 3747
pdickinson@mayerbrown.com

Megan Paul
London
+44 20 3130 3325
mpaul@mayerbrown.com

This article previously appeared in *Outsource Magazine* on May 13, 2013.http://outsourcemagazine.co.uk/governance-practical-steps-to-making-it-work/

Profit warnings are nothing new to the outsourcing industry. Looking at the end of Q1 2013, FTSE support services and FTSE software and computer services companies are again the sectors reporting the highest number of profit warnings. With the sourcing sector most vulnerable from falls in confidence due to ongoing issues in the eurozone, US and China and a decrease in government spending, it is unsurprising that this sector should continue to suffer at the hands of our difficult financial markets. However, in addition to these external factors, a failure to keep a tight grasp on governance issues could be doing far more damage. Dedicating time to due diligence at the initial stages of a project and working with your legal teams to create a solid governance structure, should help prevent problems further into the relationship.

A Strong Governance Model

A direct and honest approach about what can and cannot be achieved early in the relationship promotes trust and sets good groundwork for the development of a positive and constructive relationship.

A strong governance model allows contractual issues to be dealt with contemporaneously, promoting a stronger relationship with greater transparency, flexibility and, ultimately, sustainability.

However, there are often issues surrounding what is promised and what is (or indeed can be) delivered. If these unrealistic promises begin at the negotiation stage, the relationship is unlikely to be successful as it will be based on mistrust and a blame culture is likely to develop. A well-advised customer will challenge the service provider's pitch teams on all aspects of their solution, whilst a prepared and competent service provider will ensure it can substantiate its solution with sufficient resource dedicated to appropriate and timely due diligence, particularly in connection with IT solutions which may be dependent upon the customer's existing infrastructure or software.

A direct and honest approach about what can and cannot be achieved early in the relationship promotes trust and sets good groundwork for the development of a positive and constructive relationship.

Suitable due diligence and a mature governance model coupled with its strong implementation is — or at least should be — at the heart of any successful sourcing relationship between a customer and service provider.

Without it the parties leave themselves vulnerable to problems and complications, ranging from a loss of value in the contract, through to termination and, potentially, bad press or even litigation for non-performance or non-payment.

Suitable due diligence and a mature governance model coupled with its strong implementation is — or at least should be — at the heart of any successful sourcing relationship between a customer and service provider.

Practical Steps

The parties need to recognise the importance of an accepted common purpose at a strategic level and an understanding that both will ultimately benefit from the arrangement. Taking time at the start of the relationship to develop what a collaborative business relationship means to the parties is imperative for a successful governance model. If this is developed and adopted during the negotiation phase, a customer should feel confident it has identified a service provider with the right cultural fit for its business. A broad approach to a collaborative business relationship promotes institutional relationships, allowing each party to react intuitively and manage issues as they arise, so limiting their impact.

The customer must be prepared to retain accountability for the service, albeit whilst managing and allocating risk to its service provider. The customer cannot simply expect the service provider to understand and manage the services for it—this would be directly contrary to the collaborative business relationship. The importance of each party taking responsibility for establishing clear strategic and operative roles and activities and having capable individuals with the right authority and skills in those positions to manage (and understand) the operation of the services and monitor performance is critical. Both parties should be dedicating resources to developing skills and talent from within their own organisations for this purpose. Without suitably talented individuals managing the relationship and learning from past experience, it is possible that, aside from basic cost reduction, a customer may not fully benefit from outsourcing a function.

A good governance model allows for matters to be recorded as they arise, how they should be resolved and what steps are then taken in an effort to achieve resolution. It is essential for both parties to have a record of what issues have arisen, how swiftly they were resolved and what lessons should be learnt for the future operation of the services. This becomes even more critical where there are questions raised about performance of the service provider and where the customer may seek to demonstrate that there is a recurring problem. In extreme cases, a customer may wish to use this data to support a termination right due to persistent failures.

Whilst a governance model should be robust, it should also be capable of evolution and flexible enough to suit service demand, critical business issues and technological innovation. A well-advised customer should insist upon a mechanic to allow the operation of the services to be changed or diversified to address changing markets and evolving business demands. Connected to this is ensuring that the contract also provides for a timely approach to changes in regulation and is proactive with its responsibilities in that regard. It is in both parties' interests to ensure the flexibility of the governance model to attempt to future-proof the contract.

Conclusion

With recent reports suggesting that the UK economy is perhaps finally getting back on its feet and the claims that Wall Street is "back", there is an argument that if sourcing companies can learn from past mistakes and institutionalise strong governance models, being top of the charts for profit warnings could be a thing of the past. ◆

Mobile Application Privacy: An Overview of the Recommendations from the FTC and the California Attorney General

Rebecca S. Eisner
Lei Shen

Rebecca S. Eisner
Chicago
+1 312 701 8577
reisner@mayerbrown.com

Lei Shen
Chicago
+1 312 701 8852
lshen@mayerbrown.com

Introduction

Mobile technology raises new and unique privacy concerns due to the unprecedented amounts and types of personal information that a mobile device can collect. As a result, consumer privacy on mobile devices has become an increasingly important issue, and mobile privacy has emerged as one of the key privacy topics this year.

Mobile technology raises new and unique privacy concerns due to the unprecedented amounts and types of personal information that a mobile device can collect.

Numerous agencies and organizations—both public and private—have issued or plan to issue guidance for mobile privacy best practices. Among the most significant of these developments are the mobile privacy reports released in 2013 by both the Federal Trade Commission (FTC) and the office of California Attorney General Kamala Harris. The FTC's report, *Mobile Privacy Disclosures: Building Trust Though Transparency*, and the California Attorney General's report, *Privacy on the Go: Recommendations for the Mobile Ecosystem*, both describe best-practice recommendations for mobile privacy. The reports offer specific guidelines for participants in the mobile environment, including platform providers, application developers and third-party service providers.

This article provides an overview of the recommendations provided by both the FTC and the California Attorney General.

What Is Personal Information?

The California Attorney General defines "personally identifiable data" as "data linked to a person or persistently linked to a mobile device," including data that can identify a person via personal information or a device via a unique identifier.[1] Generally, personal information in the mobile space includes a mobile device's unique device identifier, geolocation data, a user's name, mobile phone numbers, email addresses, text messages or email, call logs, address books, financial and payment information, health and medical information, photos or videos, web-browsing history and lists of apps downloaded or used.[2]

In addition, a special subset of personal information called "sensitive information" is now recognized. The FTC views information concerning children, financial and health information, Social Security numbers and precise geolocation data as sensitive and warranting special protection.[3] Likewise, the California Attorney

General defines "sensitive information" as personally identifiable data about which users are likely to be concerned, such as precise geolocation data, financial and medical information, passwords, stored information such as contacts, photos and videos and information about children.[4]

Recommendations

Both the FTC and the California Attorney General provide specific recommendations for various participants in the mobile environment:

PLATFORM PROVIDERS

Provide Just-in-Time Disclosures: Platform providers should offer clear and understandable "just-in-time" disclosures to users and obtain a user's affirmative express consent before allowing an app to access the user's sensitive information (such as geolocation data). The FTC believes that providing such just-in-time disclosures at the time it matters to consumers (i.e., just prior to the collection of data by the app), rather than buried in a privacy policy, will allow users to make more informed choices about whether to share such data.5 The California Attorney General also recommends using similar "special notices" that would highlight any unexpected data practices (e.g., apps collecting sensitive information or personal information that is not needed for its basic functionality).[6]

Use Privacy Dashboards and Icons: Platform providers should consider using dashboards, icons and other visual cues to help users more easily and quickly recognize an app's privacy practices and settings.[7] Such privacy icons and graphics are most effective if they are standardized and users are educated about them through an awareness campaign.[8]

Provide Access to Privacy Policies: Platform providers should offer a way for users to learn about an app's privacy policy prior to the user downloading the app, so that users will be able to make a more informed decision as to whether to download the app or not. Both the FTC and the California Attorney General recommend doing this by making an app's privacy policy conspicuously accessible from the platform itself. [9] The California Attorney General already made advancements in this area with its 2012 agreement with leading platform providers, where the platform providers agreed to include in their app submission process an optional data field for the app developer to add either a link to, a copy of or a short description of the app's privacy policy.[10]

Platform providers should offer a way for users to learn about an app's privacy policy prior to the user downloading the app, so that users will be able to make a more informed decision as to whether to download the app or not.

Provide Transparency About the Platform's App Review Process: The FTC recommends that platform providers clearly disclose the extent to which they review an app before making it available for download, including any compliance checks they perform.[11] This recommendation likely stems from the FTC's complaint against Facebook, in which the FTC charged Facebook with deceiving users through Facebook's "Verified Apps" program. Facebook claimed it certified the security of apps participating in the program, when it actually did not.[12]

Develop a Do Not Track System: The FTC had previously recommended the development of a "do not track" system for web browsers that would enable users to avoid having their actions monitored online.[13] Applying this same principle to the mobile space, the FTC recommends that platform providers develop a "do not track" mechanism at the platform level so that users can choose to prevent apps from tracking their behavior across apps and transmitting such information to third parties.[14]

APP DEVELOPERS

Provide a Clear, Accurate and Conspicuously Available Privacy Policy: App developers should have a clear and accurate privacy policy for their mobile app. The privacy policy should clearly identify the app's data practices, and important terms should not be buried in long agreements or behind vague links. Among the data practices that the privacy policy should cover are how the user's data will be collected, used, shared, disclosed and retained.

An app developer should also ensure that any promises made in the privacy policy are true and accurate. The FTC has taken action against many companies that claimed to safeguard the privacy or security of their users' information but did not fulfill those promises.[15]

Finally, the privacy policy should be conspicuously available and easy to read on a mobile device. The California Attorney General recommends having the privacy policy available both from the app platform (before the app is downloaded and any data is collected) and from within the app.[16] While the small screen of a mobile device presents challenges in displaying privacy policies, app developers can consider using a layered privacy policy format that summarizes the most relevant privacy practices on top.[17]

In order to provide a complete and accurate disclosure to users, app developers should coordinate with ad networks and other third parties to fully understand the function of any third-party code being used in their apps.

It is important to note that California has a law (the California Online Privacy Protection Act, or CalOPPA) requiring mobile apps that collect personal information to conspicuously post a privacy policy, and the California Attorney General has started enforcing compliance. For example, in late 2012, the California Attorney General filed a lawsuit against Delta Airlines for failing to post a privacy policy for its "Fly Delta" app. Although a California judge recently dismissed the lawsuit on unrelated grounds, the setback is unlikely to deter the attorney general from pursuing other companies that do not comply.[18]

Understand Any Third-Party Code Included in the App: Even if an app developer provides clear and accurate disclosures about its own privacy practices in its privacy policy, app developers often include third-party code in their apps (e.g., from ad networks or analytics companies) without fully understanding what information that code may be collecting or sharing. In order to provide a complete and accurate disclosure to users, app developers should coordinate with ad networks and other third parties to fully understand the function of any third-party code being used in their apps.[19]

Limit Collection of Personal Information: App developers should build privacy considerations and protections into their apps from the beginning. This includes limiting the amount of personal information an app collects (e.g., minimizing the collection of information not necessary for the app's basic functionality), collecting or sharing sensitive information only with consent and limiting the retention of data to the time necessary to support the app's functionality or satisfy any legal requirements.[20]

ADVERTISING NETWORKS AND OTHER THIRD PARTIES[21]

The FTC recommends that advertising networks and other third parties that provide services for apps improve their communication with app developers (for example, by helping app developers understand what their code does and how it works, or by having a privacy policy and providing it to app developers). App developers would then be able to provide users with more complete and accurate disclosures.[22] In addition, the California Attorney General recommends that advertising networks avoid delivering any ads outside of the app, such as by placing icons on the mobile desktop, and use enhanced measures to obtain prior consent before accessing any personal information.[23]

Conclusion

While all service agreements include a requirement for the service provider to comply with laws, this requirement may not be sufficient when mobile apps are involved. The mobile privacy landscape is rapidly evolving, and what are considered recommendations today are likely to become requirements in the future. In addition, if a service provider is only required to design a mobile app to comply with current laws rather than incorporating privacy protections from the beginning, the adaptation of any future privacy requirements will be unnecessarily difficult. This is especially true if maintenance of the mobile app is transferred from the service provider to the company after the expiration or termination of the service agreement. To resolve this

concern, service agreements should require service providers to build in privacy considerations from the beginning and to comply with any best-practice recommendations from major public or private organizations, such as those contained in the reports from the FTC and the California Attorney General. While both the FTC and the California Attorney General have stated that the guidelines in these reports are only best-practice recommendations and not binding law,[24] these recommendations are likely a sign of things to come. The recommendations may evolve into standards, and companies that fail to heed them may become subject to investigations and enforcement actions in the future. ◆

Endnotes

1 Cal. Att'y Gen. Office, Privacy on the Go: Recommendations for the Mobile Ecosystem 6 (Jan. 2013), available at http://www.gsma.com/publicpolicy/mobile-and-privacy/mobile-privacy-principles.

2 Cal. Att'y Gen. Office, *supra* note 1, at 8.

3 F.T.C., Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers 59 (Mar. 2012), available at http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

4 Cal. Att'y Gen. Office, *supra* note 1, at 6. The European Union also recognizes certain "special categories of data" requiring extra restrictions, including data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and health or sex life. See EU Directive 95/46/EC art. 8 (1995), available at http://www.dataprotection.ie/viewdoc.asp?DocID=93&m=.

5 F.T.C., Mobile Privacy Disclosures: Building Trust Through Transparency 15, 16 (Feb. 2013), available at http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf.

6 Cal. Att'y Gen. Office, *supra* note 1, at 9.

7 F.T.C., Mobile Privacy Disclosures, *supra* note 5, at 17-18.

8 Cal. Att'y Gen. Office, *supra* note 1, at 11.

9 *Id.* at 14; F.T.C., Mobile Privacy Disclosures, *supra* note 5, at 22.

10 Press Release, Cal. Att'y Gen. Office, Joint Statement of Principles (Feb. 22, 2012), available at https://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy.

11 *Id.* at 20.

12 See Press Release, F.T.C., Facebook Settles FTC Charges That It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), available at http://ftc.gov/opa/2011/11/privacysettlement.shtm.

13 See Press Release, F.T.C., FTC Staff Issues Privacy Report, Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), available at http://www.ftc.gov/opa/2010/12/privacyreport.shtm; Press Release, F.T.C., FTC Issues Final Commission Report on Protecting Consumer Privacy (Mar. 26, 2010), available at http://www.ftc.gov/opa/2012/03/privacyframework.shtm.

14 F.T.C., Mobile Privacy Disclosures, *supra* note 5, at 20-21.

15 See, e.g., *Making Sure Companies Keep Their Privacy Promises to Consumers*, http://www.ftc.gov/opa/reporter/privacy/privacypromises.shtml (last visited June 16, 2013) (listing several legal actions that the FTC has taken against organizations for misleading them with inaccurate privacy or security promises).

16 Cal. Att'y Gen. Office, *supra* note 1, at 9.

17 *Id.* at 11.

18 See, e.g., Kurt Orzeck, *Delta Dodges Calif. Privacy Suit Over Smartphone App, Law360* (May 9, 2013, 10:09 PM), http://www.law360.com/california/articles/440392/delta-dodges-calif-privacy-suit-over-smartphone-app.

19 *Id.* at 24.

20 Cal. Att'y Gen. Office, *supra* note 1, at 9.

21 Note that the FTC report also provided recommendations for app trade associations and the California Attorney General's report also provided recommendations for operation system developers and mobile carriers. See, e.g., *id.* at 16.

22 F.T.C., Mobile Privacy Disclosures, *supra* note 5, at 24.

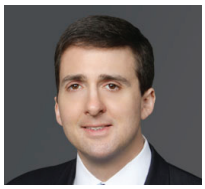
23 Cal. Att'y Gen. Office, *supra* note 1, at 15.

24 See, e.g., *id.* at 4; *FTC, Mobile Privacy Disclosures: Building Trust Through Transparency*, *supra* note 5, at 13-14.

The 2013 Cybersecurity Executive Order: Potential Impacts on the Private Sector

Rebecca S. Eisner
Howard Waltzman
Lei Shen

Rebecca S. Eisner
Chicago
+1 312 701 8577
reisner@mayerbrown.com



Howard W. Waltzman
Washington, DC
+1 202 263 3848
hwaltzman@mayerbrown.com

Lei Shen
Chicago
+1 312 701 8852
lshen@mayerbrown.com

The authors wish to thank Mayer Brown summer associate Natasha Chu for her work on this article.

In February 2013, President Barack Obama issued an executive order ("Order") outlining steps his administration will take to protect critical US infrastructure from cybersecurity threats.[1]

The Order is a directive for a collaborative effort between the government and the private sector to reduce and mitigate cyber threats and risks to the nation's critical infrastructure. It provides for the development of a process to rapidly share unclassified information with specified targets and a voluntary classified information-sharing program for eligible entities.

The Order also calls for the development of standards to identify "critical infrastructure" at greatest risk. Operators and owners of identified critical infrastructure will be confidentially notified and may request reconsideration of this status. In addition, the Order provides for the development of a voluntary Cybersecurity Framework ("Framework") outlining standards, methodologies, procedures and processes to address cybersecurity risks while balancing policy, business and technological concerns. The Secretary of Homeland Security will develop incentives to encourage adoption of the Framework.

The success of these programs will be reevaluated following publication of the final Framework to ensure usefulness and actual risk mitigation. The Order stipulates that all actions taken as a result of the Order should include the necessary precautions to protect privacy and civil liberties.

The ramifications of the Order for the private sector are still unclear and will be for some time. This article contains an overview of some of the key aspects of the Order and discusses potential impacts and challenges for companies that have critical infrastructure. Although the Order focuses on its directives on risks to owners and operators of critical infrastructure, there may be implications for industries and sectors without critical infrastructure as well. This article also considers the implications for outsourcing customers and providers.

Cybersecurity Information Sharing

The Order directs the Secretary of Homeland Security and the Attorney General to develop a voluntary cybersecurity information sharing program ("Program") that rapidly disseminates unclassified reports of domestic cyber threats to participating entities. Certain qualified and eligible participants in this Program may also receive classified cyber threat and technology information. The purpose of this Program is to

improve the efficiency and expediency of important cyber threat information sharing with private entities so they can better protect and defend themselves. One key issue for companies receiving the cybersecurity information is whether this notice will trigger any responsibilities or notification requirements under state data breach notification and security laws, particularly when the information indicates that a breach may have occurred. The extent to which a company receiving cyber threat information will be required or advised to take action on that information is unclear.

The Order directs the Secretary of Homeland Security and the Attorney General to develop a voluntary cybersecurity information sharing program ("Program") that rapidly disseminates unclassified reports of domestic cyber threats to participating entities.

Cybersecurity Framework and Voluntary Critical Infrastructure Cybersecurity Program

The Order also directs the Secretary of Commerce to oversee the development of the Cybersecurity Framework, which will include "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks."[2] Its purpose is to reduce risks to critical infrastructure and establish processes to help owners and operators of critical infrastructure identify, assess and manage risk. To facilitate the adoption of the Framework, the Order directs the Secretary of Homeland Security to establish a program of incentives to promote participation. The scope of the Framework, however, is not due until October 10, 2013.

The Order gives guidance that the Framework should be technology-neutral and should enable the development of a competitive market for products and services that satisfy its standards. If the Framework's standards are drafted broadly, it may leave significant room for variations in processes, procedures and standards, and companies may be more inclined to adopt it. On the other hand, if the Framework is more prescriptive in its approach, it could serve as a set of minimum standards that establish a degree of "reasonable care" in certain sectors of industry. In that case, companies that choose not to adopt the Framework or otherwise ignore it might face liability claims for failure to meet a minimum standard of reasonable care.

Although the Order does not articulate any performance requirements for entities designated as critical infrastructure, such entities may nonetheless feel substantial pressure to participate in the Framework. Based on the Order's language, a designated entity does not need to implement additional processes to continue business operations. However, if a cyber disaster strikes an identified entity that did not implement the Framework, and it becomes known that the entity had been identified as a critical infrastructure entity, the fact that the government gave that entity a prior warning may increase its liability.[3] Reputational harm and lawsuits may ensue. Companies that are identified as critical infrastructure entities will have to perform careful risk analyses to determine whether or not to implement the Framework and what the implications are for choosing not to do so.

Identification of Critical Infrastructure at Greatest Risk

The Order also requires the Secretary of Homeland Security to identify critical infrastructure where a cybersecurity incident could "reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security." Commercial information technology products and consumer information technology services are excepted. It is unclear which companies fall under this exception, but examples might include Google, Facebook, Microsoft and Twitter.[4] Owners and operators of identified critical infrastructure will be confidentially notified of their status; upon notification, they can request reconsideration of this designation.

At this time, we can only speculate as to which sectors of industry could be targeted by the Order. Although the President released the Presidential Policy Directive on Critical Infrastructure Security and Resilience ("Directive"), which identifies 16 critical infrastructure sectors, it remains unclear

how closely the Order's critical infrastructure list will track this one. Nevertheless, this list provides an idea of which industries and sectors the government has identified as important to national security.[5] Certain industries seem like natural candidates, such as telecommunications, media, financial services, energy and utilities.

Risks and Challenges

As mentioned above, there are two key risks created by the Order. The first risk is the potential liability that could arise in the context of existing and new breach notification and security laws resulting from the government information-sharing program. The second risk is the uncertainty about the kinds of standards the Framework will establish for critical infrastructure entities and the potential implications of failure to adopt the Framework.

The Order also creates several other risks. Companies face a potential dilemma regarding voluntary participation in the information-sharing program. While information sharing—from the government and potentially with the government—is a goal of the Program, companies that participate will need to consider privacy laws and determine whether information sharing could violate privacy laws, privacy statements or other contractual requirements. Federal contractors and subcontractors may also face rising costs since the Order mandates a review of both federal procurement policies and the merits of incorporating security standards into "acquisition planning and contract administration."[6]

Implications in the Context of Outsourcing

Entities that become subject to the Order will need to reexamine all significant service provider arrangements. This will be necessary to ensure that Framework requirements within the provider's control are included in the contract with the service provider. The Secretary of Homeland Security could also designate certain service providers managing infrastructure or information as having critical infrastructure, thus implicating client information or infrastructure that they provide and/or manage.

Companies that are not critical infrastructure operators but that outsource services to service providers that are critical infrastructure providers will need to evaluate the implications of their service provider's participation in the Program. Companies that outsource rely on their service providers not to distribute the company's information without permission. Any transfer of information by the service provider to the government as part of the Program could be a violation of the company's outsourcing contract terms. Such disclosure could also cause exposure under the company's privacy policies and could possibly cause the company to be in violation of its own customer and third-party contracts. The company could face reputational harm and liability if it were to become known that its service provider shares information with the government.

Companies that are not critical infrastructure operators but that outsource services to service providers that are critical infrastructure providers will need to evaluate the implications of their service provider's participation in the Program.

Service providers, on the other hand, could face a dilemma because their interest in complying with the provisions of their contracts may conflict with the government's goal of obtaining information to mitigate the risk of, and defend against, a cyber threat. Even if a service provider's contracts allow for government-mandated disclosure, public knowledge of any disclosure (voluntary or mandated) could have a serious impact on the service provider's reputation.

Although not the primary target of this Order, companies that do not own or operate critical infrastructure should still monitor developments under the Order, particularly with respect to service providers that may be critical infrastructure operators. Companies that do not own or operate critical infrastructure should also follow developments relating to the effect of the Framework on information security policies and practices in general. As noted above, the Framework may establish standards that will be applied across

industries and sectors, even beyond critical infrastructure sectors.

Conclusion

As the directives of the Order are published, there will be more clarity about the degree of impact it has on the private sector. It is likely, however, that private entities and service providers may face new challenges in determining how best to benefit from the Program and how to use the Framework to protect against cybersecurity threats while remaining in compliance with existing laws, regulations and contractual commitments, and limiting potential liability claims. ◆

Endnotes

1 Exec. Order No. 13636, *Improving Critical Infrastructure Cybersecurity*, 78 Fed. Reg. 11737-1144 (Feb. 19, 2013), available at https://federalregister.gov/a/2013-03915.

2 Exec. Order Sec. 7(a).

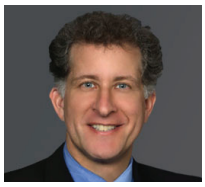
3 Paul Rosenzweig and David Inserra, *Obama's Cybersecurity Executive Order Falls Short*, The Heritage Foundation (Feb. 14, 2013), http://www.heritage.org/research/reports/2013/02/obama-s-cybersecurity-executive-order-falls-short.

4 See Zack Whittaker, *Obama's Cybersecurity Executive Order: What You Need to Know*, ZDNet (Feb. 13, 2013, 9:51 PM), http://www.zdnet.com/obamas-cybersecurity-executive-order-what-you-need-to-know-7000011221/; Andrew Webster, *White House Softens Draft Cybersecurity Orders with Exemptions for Commercial Tech Products*, The Verge (Dec. 1, 2012, 4:32 PM), http://www.theverge.com/2012/12/1/3715096/white-houses-cybersecurity-executive-order-commercial-product.

5 See Public Policy Directive No. 21, *Critical Infrastructure Security and Resilience* (Feb. 19, 2013), available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (The critical infrastructure sectors identified by the Directive are as follows: Chemical; Commercial Facilities; Communications; Critical Manufacturing; Dams; Defense Industrial Base; Emergency Services; Energy; Financial Services; Food and Agriculture; Government Facilities; Healthcare and Public Health; Information Technology; Nuclear Reactors, Materials, and Waste; Transportation Systems; Water and Wastewater Systems).

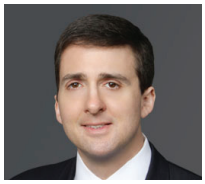
6 Exec. Order Sec. 8(e).

Rebecca S. Eisner
Chicago
+1 312 701 8577
reisner@mayerbrown.com



Jeffrey P. Taft
Washington, DC
+1 202 263 3293
jtaft@mayerbrown.com

Richard M. Rosenfeld
Washington, DC
+1 202 263 3130
rrosenfeld@mayerbrown.com



Howard W. Waltzman
Washington, DC
+1 202 263 3848
hwaltzman@mayerbrown.com

Archis A. Parasharami
Washington, DC
+1 202 263 3328
aparasharami@mayerbrown.com

Into the Breach: Managing Cybersecurity Threats in the Digital Age

PROGRAM HIGHLIGHTS

Rebecca S. Eisner
Jeffrey P. Taft
Richard M. Rosenfeld
Howard W. Waltzman
Archis A. Parasharami

In 2012 there were more than 2,600 reported incidents of data breach, more than double the number in the previous year. That figure highlights just how fast the challenge of cybersecurity is growing, with concomitant exponential growth in the cost of cyber breaches to businesses.

Mayer Brown recently hosted "Into the Breach, Managing Cybersecurity Threats in the Digital Age," featuring keynote speakers Richard Clarke, chairman and CEO of Good Harbor Security Risk Management LLC, and Mayer Brown partner Richard Ben-Veniste, whose presentation was titled "Cyber Security Threats — What They Mean for Homeland Security and Economic Growth." Messrs. Clarke and Ben-Veniste described a business community and a nation that — even after some high-profile and costly security breaches — remain ill-prepared to face the scope of the threat. While most of the measures companies are taking today are voluntary, they predict that those steps will become mandatory in the near future as federal, state and local governments contend with a growing challenge.

Joining our keynoters were panelists Jake Olcott of Good Harbor, Jonathan Cooperman of ACE North America, Larry Collins of Zurich Services Corporation and Mayer Brown partners Rebecca S. Eisner, Archis A. Parasharami, Richard M. Rosenfeld, Jeffrey P. Taft and Howard W. Waltzman. The panelists highlighted several key trends we are likely to see in 2013 and beyond, as well as some of the most important steps companies can take to mitigate the risk of cyber threats. Following are a few highlights.

Lawsuits based on cybersecurity breaches are sure to be part of the next wave of class action litigation in the United States.

Cybersecurity: The New Frontier of Class Actions and Government Investigations

Lawsuits based on cybersecurity breaches are sure to be part of the next wave of class action litigation in the United States. As with other types of class action, few cybersecurity class actions will be litigated to a judgment in favor of the plaintiffs. Still, those that survive beyond the pleadings stage could give rise to a massively expensive e-discovery process, and that potential, combined with the potential damage to a company's reputation from the allegations themselves (whether true or not), will place corporations under enormous pressure to settle.

Moreover, class actions by private plaintiffs are only one of the potential

litigation risks raised by cyber attacks; the government is watching too. At the federal level, the Department of Justice, the Federal Trade Commission and the Securities and Exchange Commission may investigate or bring actions against companies that do not adequately prepare for cyber security breaches. State attorneys general similarly may choose to intervene, as at least two state AGs did in the aftermath of deals web site LivingSocial's recent admission that hackers had breached its security and made off with large volumes of personal information.

To mitigate the risks posed by cybersecurity breaches and the potential for class action lawsuits and/or government investigations, businesses need to adopt multipronged risk management strategies. In addition to technology solutions and insurance, key components of such a strategy include drafting appropriate privacy policies (including disclaimers and limits in contracts), selecting alternative dispute resolution mechanisms, such as arbitration, and implementing PR strategies that can help reduce or avoid reputational harm.

The *New* New Disclosure Requirement: Here Comes the SEC

Corporate policies governing cybersecurity risk can reduce a company's exposure to charges from either the SEC or a litigant that a company "should have known" or "should have disclosed" its cybersecurity risks. Companies should view up-front disclosure as a preemptive strike that can limit their future liability and prevent the SEC and others from playing the "gotcha" game. The need for disclosure has increased in light of comments from new SEC chairman Mary Jo White that the SEC's 2011 cybersecurity disclosure guidance is under review. This statement, coupled with recent events, is a clear signal to the business community that the SEC plans to take disclosure very seriously and that businesses need to establish cybersecurity policies and procedures and reasonably evaluate their risks, or risk enforcement action and litigation in the near future.

President Obama's Executive Order and Its Effect on Business

President Obama's February 2013 Executive Order on Cyber Security seeks to collaboratively establish risk-based cybersecurity standards and to expand upon the Department of Defense's cyber threat information-sharing program. Yet our panelists asserted that the Executive Order's information-sharing component is inadequate because the Order lacks liability protection, which means that many companies will be afraid to voluntarily share information. The panelists agreed that only Congress can provide the protections necessary to make an information-sharing regime effective at reducing cyber threats. What's more, the Order doesn't provide companies with exemptions from privacy laws, such as the Electronic Communications Privacy Act, that are an impediment to information sharing, and that Congress must adopt these exemptions. Thus, assuming consensus can be reached on voluntary risk-based cybersecurity standards, the Executive Order was a good first step, but congressional action is essential to enhance US cybersecurity.

Corporate policies governing cybersecurity risk can reduce a company's exposure to charges from either the SEC or a litigant that a company "should have known" or "should have disclosed" its cybersecurity risks.

However, the banking industry has been generally supportive of the Executive Order because the Order recognizes the bank regulatory agencies' past and ongoing contributions in this area. Banks and other financial services firms have a long history of being targeted by criminal enterprises and defending themselves from physical and cyber threats. The bank regulatory agencies, the Financial Services Sector Coordinating Council and the Financial Services Information Sharing and Analysis Center have played an important role in helping banks identify threats, protect critical infrastructure and share information about cyber threats.

Cyber Vulnerabilities — Identifying Legal Risk and Approaches for Risk Mitigation

Conducting a security assessment is the best way to determine whether and how a company is protecting its most valuable information assets. A security assessment and implementation of reasonable

security measures after undertaking the assessment also provide some defensive protection not only around security threats, but also against follow-on claims and liability. Many laws and regulations dealing with data protection require that companies use *reasonable efforts* to protect the security of their data, consistent with the risks associated with the type of data. A security assessment can help in making the argument that a company has indeed taken reasonable efforts to protect its information.

Conducting a security assessment is the best way to determine whether and how a company is protecting its most valuable information assets.

A security assessment often requires contracting the services of a qualified consultant who can help gather business documents and validate technical processes. However, a security assessment should be run by a company's legal department, not by the consultant. Lawyers, working with the consultant and the business team, can help to ensure that the findings of the assessment are carefully captured and stated. Since perfect privacy and security compliance are not possible, a company must identify remediation steps in areas where it has determined the risk/benefit ratio is the greatest. It is also important in any assessment to ensure that the written record of the assessment does not contain inaccurate statements, speculation or recommendations that are practically difficult to implement or are commercially unreasonable to attain. In overseeing the assessment, lawyers can interpret the legal standards and assist the consultant and business teams in putting together an attainable set of security practices and policies that will better protect the company's valuable information assets.

Monitoring Third Parties and Supply Chain Vendors

Companies need to monitor third parties and companies in their supply chain as part of any security and privacy compliance program, as both of these represent major areas of vulnerability in security and privacy compliance. For the most-critical third-party vendors, security assessments should be performed, including an assessment of protocols vendors have in place for responding to a security breach. Critical vendors should also be considered in a company's incident-response plan.

To ensure the ability to conduct assessments of such vendors and suppliers, a company should use a contract that requires the cooperation of the third party in ongoing security assessments, audits and incident management, including security breaches. The contract should require the vendor to remediate known security vulnerabilities identified after an assessment, audit or security incident. The vendor should be required to notify the company immediately in the event of a known or suspected security incident, and should cooperate with the company in any resulting investigations, claims and government actions. Whether to notify individuals and government authorities should be a decision made by the company with respect to its data, not by its vendor. The contract should also allocate financial responsibility for notification costs, remediation of identified security failures, follow-on costs of investigations and settlements, resulting claims from third parties, and even credit monitoring and other similar consumer response actions, such as call centers to answer questions from individuals about the incident. ◆

BRAD PETERSON

Partner

Brad Peterson, a partner in the Chicago office, focuses on outsourcing, joint ventures, strategic alliances and information technology transactions. Brad has represented customers in dozens of large outsourcing agreements, including outsourcing finance and accounting, procurement, human resources, IT infrastructure, applications development and maintenance and other functions. Brad has also represented information technology buyers in hundreds of technology transactions, including cloud computing, software licensing, software development agreements, hosted services agreements, and ERP implementation agreements. With a background in the IT industry, an MBA from the University of Chicago and a JD from Harvard Law School, he provides practical, business-oriented advice on contracting for technology and services.

GREGORY MANTER

Partner

Gregory Manter is a partner at Mayer Brown in Chicago and a member of the Business & Technology Sourcing practice. He represents clients in a wide variety of information technology and business process outsourcing transactions and other information technology licensing and development transactions. He has represented customers in numerous software implementation agreements, including several large ERP implementation agreements.

ROBERT KRISS

Partner

Robert Kriss, a partner in the Chicago office, has represented some of the world's largest Internet and technology companies in commercial and class action litigation. He began representing Internet-based companies in the late 1990s, when he successfully defended America Online in over 60 class actions arising from consumers' alleged difficulties connecting to AOL. Since then, Bob has successfully defended numerous consumer class actions involving a wide variety of Internet-based marketing and billing practices and has represented both suppliers and customers in commercial disputes involving information technology outsourcing and new system implementation. He also has assisted companies in investigating and remediating data breaches and in establishing privacy policies. Bob recently was recognized by Martindale Hubbell as among the "Top Rated Lawyers of Technology Law."

REBECCA EISNER

Partner

Rebecca Eisner, a partner in the Chicago office, serves on Mayer Brown's Partnership Board. She focuses her practice on technology and business process outsourcing and sourcing, information technology transactions, privacy and security. Her experience includes complex global technology, licensing and business process outsourcing transactions, including IT infrastructure and licensing, cloud computing, applications development and maintenance, back office processing, ERP implementations, finance and accounting, payroll processing, call center, HR, technology development, system integration and hosting. She regularly advises clients in Internet and e-commerce law issues, complex data protection and data transfer issues, privacy compliance issues, and electronic contracting and signatures. She is a frequent writer and speaker on outsourcing, cloud computing and privacy and data protection topics. Additionally, she is the co-chair of the Data Security Chapter of the International Association of Outsourcing Professionals.

LEI SHEN

Associate

Lei Shen is an associate in the Business & Technology Sourcing practice group in Mayer Brown's Chicago office. Lei focuses her practice on privacy and security, technology and business process outsourcing (including information technology, finance and accounting, procurement, human resources, and customer relationship and call centers), and information technology transactions, privacy and security.

HOWARD WALTZMAN

Partner

Howard Waltzman, a partner in the Washington, DC office, focuses his practice on communications and Internet law and privacy compliance. He represents some of the nation's leading communications service providers, manufacturers and trade associations in regulatory, compliance and legislative matters, including with respect to Internet and wireless services, privacy, video programming and communications-related homeland security. He also represents investors on these and other communications-related matters.

DANIELLE FISHER

Associate

Danielle Fisher is an associate in the Washington, DC office of Mayer Brown's Business & Technology Sourcing and Corporate & Securities practices. She advises clients in various industries in the areas of technology and business process outsourcing. She also focuses on corporate transactional law with a special emphasis on transactions involving the development, licensing and distribution of technology.

DANIEL MASUR

Partner

Daniel Masur, a partner in the Washington, DC office, has represented national and international clients in a broad range of onshore, near-shore and offshore information technology and business process sourcing transactions involving global and niche outsourcing providers, offshore captives and various hybrid structures. Prior to joining Mayer Brown, Dan served as General Counsel of I-NET, Inc., a provider of outsourcing services. Dan is recognized as one of the leading lawyers in the outsourcing field by Chambers Global, Chambers USA, Legal 500 and Best Lawyers in America.

PETER DICKINSON

Partner

Peter Dickinson is head of Mayer Brown's Corporate group in the UK and a Firm Practice Leader in Mayer Brown's global corporate and securities practice. Peter's practice focuses on mergers and acquisitions, joint ventures and other significant commercial transactions including, in particular, large-scale multi-jurisdictional outsourcing projects.

MEGAN PAUL

Senior Associate

Megan Paul is a senior associate in the Corporate & Securities practice of the London office. She undertakes a broad spectrum of transactional corporate and commercial work, focusing primarily on international and domestic private equity and venture capital transactions and outsourcing. Megan has significant experience with outsourcing transactions, acting on behalf of suppliers and customers across multi-jurisdictions and in a variety of industry sectors. She also has experience in domestic and international mergers and acquisitions and large corporate reorganizations.

JEFFREY TAFT

Partner

Jeffrey Taft is a regulatory attorney whose practice focuses primarily on privacy and data security, banking regulation, consumer payment systems and consumer financial services. He has extensive experience counseling financial institutions, merchants and other entities on various federal and state consumer credit protection issues, including compliance with the Gramm-Leach-Bliley Act (GLB Act), the Fair Credit Reporting Act , the Electronic Fund Transfer Act, the Right to Financial Privacy Act, state and federal unfair or deceptive practices statutes and state privacy and data breach laws and regularly assists financial services firms and other companies with their development, implementation and review of privacy and information security programs designed to comply with the GLB Act, state privacy and data breach laws and industry standards.

RICHARD ROSENFELD

Partner

Richard Rosenfeld is co-lead of Mayer Brown's US Securities Litigation & Enforcement group working from both the Washington, DC and New York offices. Richard has nearly 20 years of experience practicing in the securities field, including more than a decade in high-level government regulatory and enforcement positions. He represents financial institutions, funds, companies and individuals in a variety of business, regulatory and compliance issues. He advises on transactions, policies and procedures, investigations, regulatory enforcement and litigation before the SEC, FINRA, other financial services regulators, including states, and the US Department of Justice. Richard has substantial securities litigation experience in the federal courts, in addition to leading internal investigations and advising clients on regulatory compliance, corporate governance and other SEC-related issues.

ARCHIS PARASHARAMI

Partner

Archis Parasharami is a co-chair of the firm's Consumer Litigation & Class Actions practice. He defends businesses in class action litigation in federal and state courts around the country, with a focus on strategy issues, multidistrict litigation and critical motions seeking the dismissal of class actions or opposing class certification. He also has helped businesses achieve settlements on highly favorable terms in significant class actions. Archis also has substantial experience in drafting and enforcing arbitration agreements for companies that require individual arbitration in place of class action litigation.

DEREK SCHAFFNER

Senior Associate

Derek J. Schaffner is a senior associate in the Business & Technology Sourcing practice of the Washington, DC office and represents clients in complex information technology and business process outsourcing transactions. Prior to practicing law, Derek spent a decade in the technology industry as a corporate controller at Microsoft and Xerox. While at Microsoft, Derek served as the financial executive for the Global Accounts organization and led business modeling activities for the redesign of Microsoft's enterprise business. While at Xerox, Derek oversaw numerous financial system implementation projects, including the development of the company's first intranet and a worldwide financial reporting consolidation platform. He began his career as a management information consultant at Accenture where he helped develop and implement manufacturing and retail system solutions.

LINDA RHODES

Partner

Linda Rhodes, partner in the Washington, DC office, focuses her practice on complex commercial transactions, with a primary focus on business and technology sourcing. She has represented a wide spectrum of clients, including large multinational corporations, in a variety of industries, such as information technology, telecommunications, pharmaceuticals, health care, financial services, insurance, energy, chemicals and consumer products. She has substantial experience in leading contract negotiations, bringing complex transactions to successful closure and effectively managing the international aspects of global transactions.

About Mayer Brown

Mayer Brown is a global legal services organization advising clients across the Americas, Asia and Europe. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest banks. We provide legal services in areas such as banking and finance; corporate and securities; litigation and dispute resolution; antitrust and competition; US Supreme Court and appellate matters; employment and benefits; environmental; financial services regulatory & enforcement; government and global trade; intellectual property; real estate; tax; restructuring, bankruptcy and insolvency; and wealth management.

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.